universität wien

MASTERARBEIT

Titel

Challenges in Implementing Information Security policies

Verfasser

Andreas Reichard

angestrebter akademischer Grad

Diplomingenieur

Wien, 2010

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienblatt:	Wirtschaftsinformatik
Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

Index

Acknowledgements

In the process of writing this thesis I encountered a number of people whose support in this project was not only helpful, but inspiring especially in periods when my motivation was somewhat lacking. To these people I owe much gratitude and, while I hope I have not omitted anyone, would like to mention them in the following, in no particular order:

My parents, *Dipl.-Ing. Dr. Johann Reichard* and *Dr. Beatriz Reichard*, for their support during the time of my studies and beyond.

Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr, not merely for the supervision, but for his generous understanding, patience and advice regarding not only my thesis, but other matters as well.

Prof. Anselmo del Moral Bueno, for his support with my thesis during my stay in Bilbao at the University of Deusto, Bilbao.

Pablo Garaizar Sagarminaga, for his support during my stay in Bilbao at the University of Deusto and his patience with my questions regarding Linux and network security.

Liher Elgezabal, for his generous support during my stay in Bilbao.

Dr. phil. Markus Rheindorf, for linguistic corrections.

To certain individuals who chose to remain anonymous, for the time they took to grant me valuable insights into practical aspects of Information Security and the implementation of the corresponding policies.

1. Introduction

In today's world information has become an asset of often considerable value. In a number of contexts, e.g. politics, science, but also business and commerce, enabling or denying access to specific information can have a significant impact on people, companies, even whole governments. With technical advances in the development of infrastructure designed for processing and distribution of information, it becomes increasingly easy to spread this information among large numbers of recipients through various distribution channels. The rapid pace at which this can happen, along with decreasing prices for the required infrastructure, raises a number of concerns.

It is safe to say that practically no business can nowadays survive without the use of some kind of infrastructure to process information and make it available to certain individuals. Whether this is a single, non-networked computer workstation containing salary data or a whole network infrastructure, the principles remain the same: Among employees, with business partners or costumers, the sheer existence and possible sharing of business-related information and the circumstances under which access to this information may be granted or denied is a topic that cannot be ignored. The main reason for this necessity is that this information becomes part of a company's assets the moment it is brought into existence as something that is distributable.

Consequently, *every* kind of information carries a specific value. The exact amount of that value depends on factors such as its content, confidentiality, owner etc. In some cases, especially in business, this amount can be expressed as a monetary value, e.g. if that information is sold 'as it is' (e.g. a software license registration number that can be obtained over the Internet using a credit card for payment) or if its impact in a specific context is well-known to the people involved and/or responsible for its distribution (e.g. news that can affect the market stock of a company). In other cases, this may prove to be more difficult, as the impact and consequences of information being distributed into certain hands are hard to predict, let alone expressed as a monetary value.

It is that uncertainty about possible consequences of sensitive information getting into the wrong hands that has forced companies to devise comprehensive plans on how to prevent this from ever happening. This includes adequately dealing with information – not only highly sensitive information, but information in general – in a way that does not constrain business processes unnecessarily, while still protecting the information as a valuable asset from illicit access. All these concerns fall into the field of Information Security.

Recognizing the danger of information exposure, many businesses have invested considerable time and effort into the creation of an Information Security program. The creation of such a program is a complex task in its own right, worthy of recognition. The effort devoted to such a program, however, does not guarantee the efficiency of its application, i.e. the crucial issue of whether the people affected by it will also comply with it and, if they do, to what extent.

Investing substantial effort into the design of an Information Security program without sufficiently acknowledging how coworkers will be affected will likely lead to a large gap between the conception and application of such a program. In a worst case scenario, this may even render the entire Information Security program useless if people do not recognize it as an overall benefit for them or the company. On the contrary, if they see little or no benefit in compliance, accomplishing their day-to-day tasks in the most efficient and time-saving manner will receive the highest priority instead of Information Security. Since the measures put in place by an Information Security program to protect valuable information will most likely stand in their way in one way or another, this usually involves violating a number of those measures, thereby endangering valuable information.

The problem that presents itself in such a case is not so much the sheer act of active non-compliance by an employee with a company's efforts to protect its information assets. As unacceptable as such behavior may be, and as harsh as the consequences must be, those responsible for Information Security must look at the bigger picture in order to recognize the motivation behind such actions. Some form of disciplinary action against violations of Information Security may, depending on the gravity of the acts committed, be part of such consequences. More importantly, however, it is paramount to reveal the reasons why an employee does not seem to understand the necessity of the measures he or she was trying to circumvent in order to get work done more quickly or probably just more conveniently. In most cases, the reason behind such behavior is a simple lack of awareness. Furthermore, the reason for the grave importance of understanding this is that one can never be sure how many other employees feel the same way about the Information Security measures that have been violated. Any one of these employees is therefore a potential Information Security risk as they might have taken the same steps as the original violator, possibly for the same reasons and it is probably only luck that they haven't done so already. This alone is reason enough to take an honest look at what they were trying to do and, more importantly, why. In other words, such an incident – again, depending on its gravity – should present sufficient reason to question whether the design of an Information Security program is flawed, creating a discrepancy between the implementation of that program and its intention.

This thesis therefore recognizes that there is a substantial difference between the *design* and the *implementation* of an Information Security program. It is that difference that is responsible for the existence of a possible gap between conception and application of an Information Security program. This gap leads to incidents as described above, in which an Information Security program may have been put in place, but is not being followed and therefore partially ineffective. Any company that values its information, which should literally entail *any* company in existence, must take such matters seriously, even if that means reviewing the conceptions that originally guided the implementation of an Information Security program.

Considering the efforts in terms of budget and manpower that are devoted to the design and implementation of an Information Security program, probably not all managers would, in a situation as described above, agree to the necessity of 'going back to the drawing board'. Some might not even be willing to grant such budget in the first place for something they probably have not understood up to that point. The fact remains, however, that an ineffective

Information Security program is an Information Security leak by itself and a crucial one at that, because it offers a false sense of security where in reality there is a lack of the same. It is therefore imperative to convince management of the need for an effectively implemented and functioning Information Security program, and of the dangers entailed in believing that a company relying on the secure handling of its information assets can realistically operate without one.

This thesis acknowledges that there are a number of publications on the subject of how to devise good security policies. The current de facto standard for this in Austria is the 'Österreichisches Informationssicherheitshandbuch' (Bundeskanzleramt Österreich [04.06. 2010]). Another excellent summary of security policy development is given in 'Management of Information Security' (Whitman, Mattord 2007 [2004]: 107). However, the area defined by the issues that may arise in the actual process of implementing these policies that affect their efficiency has not been addressed adequately to date. In light of this shortcoming, those responsible for the implementation of Information Security within a company are left with the following pressing questions:

- **How can the gap between conception and application be reduced, or, more to the point, how can Information Security be communicated to people, employees and management alike, so as to make them recognize the overall value of Information Security – both for them personally and for the company they are working for?** Only through such understanding, i.e. awareness, can compliance with an Information Security program be achieved, making it work as intended by its design.

- Besides coworkers, **how can management be convinced of the importance of an effectively implemented and functioning Information Security program, so as to grant the necessary budget to design, implement and maintain one?**

This thesis can be of help with these objectives by proposing answers to the above questions. Although the successful implementation of an Information Security program is closely related to its design and creation, it must be pointed out that this thesis is not focused on the *design* of such a program per se. Due to the nature of this close relation, this thesis may indeed offer additional insight into the design of an Information Security program. Its main topic, however, is overcoming any obstacles during the implementation phase that might appear during the application of an Information Security program and thereby reduce its efficiency. Doing so will not only allow one to maximize the acceptance of an Information Security program on part of the people affected by it, because it enables them to see it as an effort to protect information as a common asset, but also get the necessary budget to design, implement and, most importantly, maintain an effective Information Security program.

The achievement of such a goal is no small issue, as resistance against change is generally something that always was and probably always will be part of human nature. Since the implementation of an Information Security program within a company goes along with changes in work processes that have probably, depending on its current view on Information Security, been established for several years, getting used to these changes will require a high

level of cooperation from the people involved. This cooperation can only be the result of a sufficiently high level of awareness, starting with management and running top-down through the whole company's hierarchy, so as to try to ensure compliance with an Information Security program by each and every individual within the company.

2. The value of information

2.1 Information assets

Every company has assets which represent a specific value. A company's assets are its infrastructure, buildings, workforce, etc. The loss of any of these assets represents a loss of value to the company that owns them. This loss becomes even greater if they are connected to the company in some specialized way. The higher the grade of specialization that an asset has in connection to its owner, the more valuable it becomes not only to him or her, but to anyone interested in obtaining it.

By that definition, a company's information is an asset specialized in many ways. While the content of such information can vary greatly and, with it, the value it has for any given person obtaining that information, it should be noted that different kinds of information can have different values for different individuals. Also, for *every* kind of information there is someone for whom this information has value. This is true even for seemingly unlikely cases, meaning that information that is regarded as practically worthless by one person can have some kind of value to another, depending on the person that wishes to obtain it or has already done so. As a consequence, there simply is no 'unimportant' information. In the interest of safe-guarding a company's assets, every kind of information should therefore be protected against unrightful access and possible exploitation, since it is impossible to predict in what way this information may be used once it has been obtained.

2.2 Information threats: Social Engineering, virtual identities and identity theft

Seemingly harmless information in the hands of a person who knows how to use it can still cause great damage to a company. So-called 'Social Engineers', by using linguistic and psychological methods, are specialized in extracting this kind of information from unsuspecting employees. Their victims, unaware of the ways in which even such information can be used by such specialists, often do not see anything wrong with sharing it or are led to believe that it is alright to divulge it within a scenario that was specifically created by a Social Engineer to lead them to that conclusion. However, such information can later be put to use to harm a company as it can be planted specifically in a chain of actions that can ultimately lead a skilled Social Engineer from seemingly unimportant information to information that has significant monetary value. Dorothy E. Denning offers the following definition of this practice: "Social Engineering refers to operations that trick others into doing something they would not do if they knew the truth, for example, giving out a secret password or sensitive corporate information. Any medium that provides one-to-one communications [sic] between people can be exploited, including face-to-face, telephone, and electronic mail" (Denning, 1999 [1998]: 111).

Various books and publications have been published on the topic of Social Engineering, among them two books by former hacker and Social Engineer Kevin Mitnick (i.e. Mitnick, 2002, 2006). In the context of Information Security, Social Engineering is a highly sensitive matter as the targets of such psychology-based attacks often act with good intentions towards their company, yet opening the way for a Social Engineer to exploit that intention and damage the company. Possible contexts in which this can happen are corporate espionage, blackmail as well as privately motivated enrichment, e.g. via identity theft, which is one of the most wide-spread methods of application for stolen information.

Through the spread of online communities, e-commerce etc., many people have created for themselves a number of virtual identities. The reason for the existence of such virtual identities, from the perspective of an institution (e.g. a company offering to do e-commerce), is to have a representation of the identity's owner with whom it can communicate and do business regardless of the owner's current geographical location. A virtual identity thus serves as an interface between those two parties. For the owner of such an identity, on the other hand, this means that, by using his or her virtual identity, he or she has access to the institution's offers and services, also regardless of where this institution is located (at least in a geographical sense; other aspects such as different legislations and how this affects such a cross-country or even international relation still have to be taken into account). The only conditions for the use of such an identity are therefore a) the mutual agreement of both parties that business between them will be conducted via use of that identity and b) access to that identity by its owner. The latter can usually be equated with having access to the Internet, since most virtual identities nowadays operate through the use of this medium.

The existence of a virtual identity means that in the eyes of an institution that conducts business by handing out virtual identities to its costumers, such an identity *is* virtually the owner. Anything that is done via use of this virtual identity is traced back to its owner and deemed to have happened with his knowing and compliance. The growth rate of e-commerce over the Internet has proven that this concept has helped to open markets throughout the world, enabling companies and costumers to gain access to each other and do business regardless of geographical distances. Unfortunately, this has also introduced a set of problems, a crucial one being the illegal use of a virtual identity by another person, i.e. someone other than the original owner of that identity. This constitutes the crime of 'identity theft'. This represents a problem insofar as, from the point of view of the institution handing out these identities, any action committed through the use of a virtual identity is seen as having been committed by the person to whom this identity is registered. Obtaining such a virtual identity by illegal means and using it for criminal activities is therefore a way to frame someone else (the original owner of the virtual identity) for actions that this person did not, in all actuality, commit, while most likely benefiting from it in some way. The above scenario represents a worst-case scenario, whereas unwanted consequences of identity theft may also be caused, e.g. by the use of a virtual identity by a close family member ordering items under the name of the identity's original owner. In this case, the original owner might later find him- or herself wondering when such an order was placed because he or she cannot remember ever having done so.

A scenario in which a 12-year-old orders a movie DVD rated NC-17 (meaning that no children under the age of 17 are allowed to watch such a movie) from an online store by using the virtual identity of his or her father is not only realistic, but also demonstrates one of the major problems in the use of virtual identities. This problem stems from the fact that, by design, any virtual identity should be used by one person only, i.e. the person who originally intended to be identifiable through that identity by the identity's supplier, i.e. the institution handing out virtual identities in order to conduct business with them. However, as in the case of the 12-year-old, implementing that design in reality can prove difficult, as there are simply no ways to enforce this effectively. It is left to the individuals themselves to handle their identities in a responsible manner, in their own interest. Unfortunately, this often means that these individuals, due to ignorance, imprudence or carelessness, risk their virtual identities in a way that makes illegal access to them easily possible. In the above scenario, simply not logging out from an online store will allow the father's identity to be 'stolen' by his child using the same computer shortly after.

The example discussed above is one of the less dire cases of identity theft. Other ways by which identities are stolen these days are numerous and effective, sometimes very creative and all too often lead to far more drastic consequences than in the example above. Among these, one method of identity theft is of particular interest: so-called 'phishing'. That is not only because it is so often successfully practiced these days, but also because it represents a good example of a typical Social Engineering tactic being used with the intent to gain valuable information, in this case a virtual identity. The Anti-Phishing Working Group (APWG) describes phishing as follows: "Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc." (APWG as quoted in McClure/Scambray/Kurtz, 2005 [1999]: 623).

As a criminal phenomenon, the theft of virtual identities is one of the most recent developments caused by the spread of Internet access throughout the world. As more and more business is conducted through this medium and more people gain access to the services provided by companies, the more interesting and rewarding becomes the prospect of obtaining a number of virtual identities from a criminal perspective. The problem of identity theft, however, is not solely Internet-based. Where people are involved, there are numerous situations in which they themselves present their virtual identities to others in order to gain access to restricted information (bank account numbers, pin numbers, credit cards etc.). Even the theft of a credit card with the intent to pay with it, without being the original owner of that card, represents the crime of identity theft for a simple reason: The possession of this card, rightfully or not, is considered proof for the identity of the original owner in many cases (e.g. in every situation in which no additional form of identification is required). Therein lies another problem with virtual identities: How to prove one's identity and therefore the right to use a virtual identity for its rightful purpose? In case of credit cards, some institutions demand additional identification like seeing a driver's license or passport before accepting a credit card as a valid virtual identity (this usually happens when picking up flight tickets that have been paid via use of a credit card from a check-in counter). Other forms of additional identification for virtual identities include biometric sensors, pass phrases, access codes, pin

numbers, secret code words and answers to pre-defined questions (e.g. ‘what is my mother’s maiden name?’; note, however, that this kind of verification is not recommended as it is highly vulnerable to Social Engineering attacks). In other cases, however, such additional verification of one’s identity is not required; it is simply taken for granted that whoever presents a virtual identity is also its rightful owner (e.g. when paying with credit card in restaurants).

In every one of these situations, there exists the possibility of stealing the identity through which a person identifies itself to another person or institution and then posing as the original owner of that identity. These cases are also considered identity theft, though not Internet-based as they happen in the so-called ‘real world’. In case of virtual identities used over the Internet, performing additional identity checks in order to guarantee the rightful use of a virtual identity proves difficult, as could be seen in the above example of a 12-year-old child stealing his or her father’s virtual identity to buy items that would restricted for him or her for legal reasons. Most attempts to verify one’s identity (and consequently the right to use a virtual identity) over the Internet are based on presenting information that, one way or another, can be stolen using Social Engineering tactics. As long as the owners of that information and their virtual identities are not sufficiently aware of either the value of a seemingly trivial kind of information (e.g. a pet’s name that is used for verification of an identity) and consequently guard it accordingly, or of the ways that such information can be obtained using Social Engineering tactics, attacks of this kind will continue to succeed in accessing that information and stealing the virtual identities connected to it.

3. Information Security policies

3.1 What are Information Security policies?

In his book 'Building an Information Security Awareness Program', Mark B. Desman describes Information Security policies as follows: "Your [the reader's] objectives in preparing policies and procedures is to present a picture as to how the company views its information assets, what each employee's responsibility is with regards to protecting those assets and how to go about doing so" (Desman, 2002 [2001]: 47).

The objective underlying Information Security policies is thus, first and foremost, to have a clear picture of a company's view on Information Security for everyone within the company, from top to bottom, to see, turn and refer to in times of need. Moreover, Information Security policies should offer not only theoretical guidance ('what do we need'), but also present practical guidelines and procedures for the actual implementation ('what needs to be done and how to do it') of Information Security within a company, so as to support the company's view on Information Security throughout all of its processes.

3.2 Applications of Information Security policies

Applications of Information Security policies, their advantages and some of the major reasons underlying the necessity of having Information Security policies within a company are presented in the following.

3.2.1 Clearance of subjective decision-making

The value that information holds in general has already been discussed. However, sometimes the value attributed to one specific piece of information may be the result of a subjective decision made by one individual. Based on that decision, that information will be treated with a specific level of confidentiality by this individual and, possibly, passed to another. As such a subjective decision varies from person to person, so does the level of confidentiality. In an environment where Information Security is taken seriously, such a large margin of variation is not acceptable. This simple fact necessitates a set of documents, rules and procedures – which are written down in order to eliminate any ambiguity as to how information is to be treated – that determine both the level of confidentiality and the people who shall have access to an information asset. Taken together, such a set of documents constitute the Information Security policies of a company.

3.2.2 Document of reference on legal issues

The existence of Information Security policies should be accompanied by the full cooperation of the employees affected by it. As this sometimes requires changing people's awareness, way of thinking and established work processes to a significant degree, such cooperation is not

always self-evident due to some people's general tendency to resist change. It is therefore a common practice to have all new employees, when they first start working at a company, attend an Information Security class during a company's Orientation days which was especially designed for newly recruited employees. At the end of this class, they sign an agreement stating that they have read and understood the company's view on Information Security and its policies and will comply with them. With such an agreement, it is easy to refer to a company's Information Security policies in case of a violation because this violation implies that this agreement has been broken by the employee in question. By reminding an employee in violation of such an agreement that he or she has a) indeed been pre-informed of the company's view on Information Security (so there is no deniability) and b) confirmed that he/she has indeed read and understood the company's view on Information Security (i.e. it's Information Security policies) by signing an Information Security agreement, disciplinary actions or even legal prosecution can easily be pursued as a consequence of such violations.

But these are not the only cases in which Information Security policies provide an important document of reference for a company's view of Information Security. Due to regulative requirements, certificate audits or just internal reasons, such a document provides auditors with a point of reference on a company's actual or intended stance on Information Security. External auditors will use a company's Information Security policies to review whether a) they still comply with the current state of the law or fulfill the requirements to hold a certain certificate, while also – if they do – b) review the company's actual handling of information within its work processes to see if it complies with the company's declared Information Security policies (and thus, by implication, also current law or the requirements for a certificate in question). Internal auditors will do the same in hope of finding any weaknesses before external auditors do so in a subsequent audit, so as to prepare the company for an external audit or simply to make sure that the current level of Information Security within the company is appropriate.

3.2.3 Manifestation of Information Security responsibilities

One of the major objectives of Information Security policies is to leave no room for ambiguity about Information Security issues within the processes of a company's business or anyone involved. With the policies at hand and for everyone to see, every individual within a company, from top to bottom of its hierarchy, should know exactly how to act in any situation involving Information Security issues. In order to achieve that goal, responsibilities concerning Information Security must be clearly defined. For the purpose of this thesis, Information Security responsibilities are grouped into the following three categories: general Information Security responsibilities, specialized Information Security responsibilities and administrative policy responsibilities. The following figure visualizes their relations to each other.

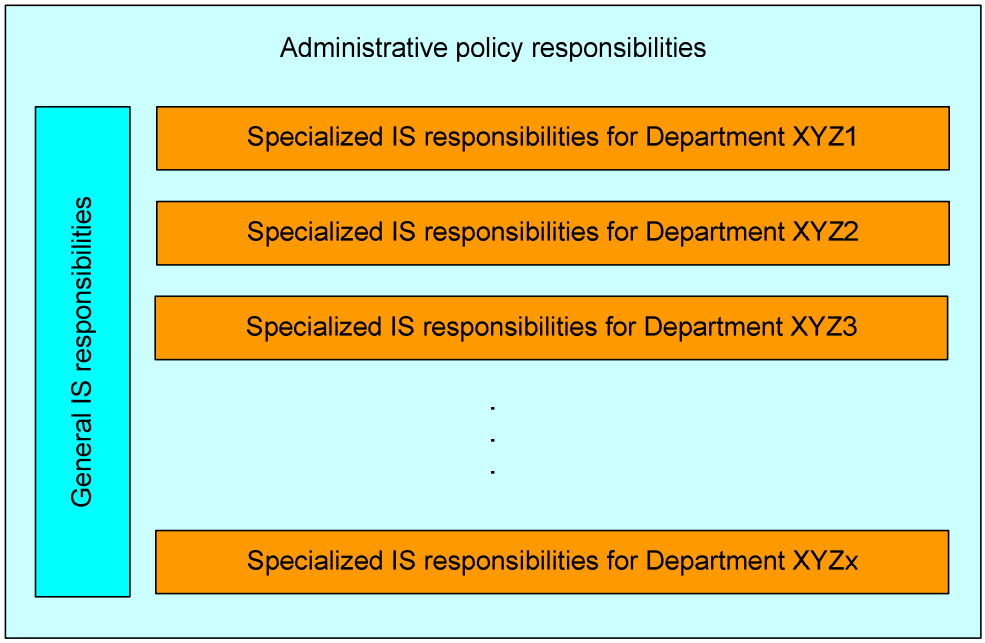

Fig. 1: Information Security responsibilities for x departments of a company and their relations to each other

General Information Security responsibilities are responsibilities that apply to any individual that is expected to follow the Information Security policies of the company related to him or her. Within any company, this applies from janitor to CEO without exception. Outside of a company, these responsibilities include business partners, contractors, i.e. any person that, during its day-to-day work, may come into contact with the respective company's information assets. Due to the broad range of work fields that these responsibilities have to cover, they are usually of a general nature. This means that they intentionally lack elaboration as to Information Security within specific work fields, so as to present the company's general view on Information Security and define what its employees can do to contribute to it.

Specialized Information Security responsibilities elaborate on certain Information Security issues that may come up in specific work fields or positions within a company. Contrary to general Information Security responsibilities, which offer a general idea of a company's view of Information Security and its expectations of its employees, specialized Information Security responsibilities should be specifically designed for a particular field of work or department and should contain answers to all Information Security-related questions that may present themselves in any employee's line of work and cannot be answered by the general Information Security responsibilities. These responsibilities therefore differ between departments, as e.g. human resources (HR) may encounter other Information Security issues than public relations (PR). Specialized Information Security responsibilities must therefore exist for all departments as well as for outside relations such as business partners or contractors. It is equally important to note that, although specialized Information Security responsibilities exist for all departments, it is not necessary to create an information overload by sharing all this specialized information with every department. General Information Security responsibilities need to be devised in such a way as to give any department an accurate idea of what the specialized Information Security responsibilities of another department might look like without actually detailing them exactly. Of course, the documentation for each department's specialized Information Security responsibilities is

available to everyone, but in order to prevent an information overload, it suffices that each department knows about its own specialized Information Security responsibilities.

Administrative policy responsibilities are about the responsibilities in the establishment, review, enforcement, adherence, update and maintenance of Information Security policies and all administrative Information Security efforts within a company. These responsibilities specifically declare which persons or departments are responsible for each one of the aforementioned points of interest. It is important to understand that these responsibilities are not simply the specialized Information Security responsibilities of the department responsible for administering Information Security efforts within a company (which exist separately), but instead declare the responsibilities for administrative functions concerning Information Security both within the company as well as for its outside relations.

3.2.4 Scope of Information Security policies

Depending on the size of the company and its field of operation, the scope of Information Security policies may differ between companies. Generally speaking, when determining the scope of Information Security policies, at least two areas must be taken into account: Internal and external communications. Internal communications are all transfers of information that fall within the range of the company itself, i.e. between internal departments. External communications are all transfers of information that go beyond a company's borders, i.e. with business partners, outside contractors, government agencies, costumers or generally any kind of relation with someone outside the company.

It is vital to understand that in this context the borders of a company are in no way limited by its geographic location, but by the range of communication that it can reach using any kind of information medium at its disposal. However, geographical locations do matter from a legal point of view, as the crossing of a national border usually entails the confrontation with a different legislation. Since Information Security policies rely heavily on legislation, being bound to it by necessity, the fact that they have to deal with two or more different legislations needs to be taken into account as well.

3.2.5 Definition of terms

One very important reason for the existence of Information Security policies is preventing mistakes in handling information assets that are based on two different interpretations of the same term. That is, the word 'guideline' may have differing meanings for two different individuals. Many such mistakes are the result of different perspectives based on misunderstandings of terminology between employees in the handling of information assets. Such mistakes can be avoided by providing employees with clear-cut terminology to be used in every kind of communication.

The definition of terms in Information Security policies will be covered in more detail in chapter 3.3.5.

3.2.6 Classifications

For similar reasons as mentioned above, Information Security policies should contain a list of clear classifications and their explanations, e.g. detailing the sensitivity of information assets, access rights, incident gravity, risk levels etc.

That is, the classifying word ‘grave’ may have a different meaning for two different employees when used to describe an Information Security incident with costumer impact. Such a misunderstanding can easily be avoided by putting the term ‘grave’ into the classifications section of the company’s Information Security policies along with an explanation of the conditions under which an Information Security incident is to be labeled as ‘grave’ in case it involves costumer impact.

Classifications will be covered in more detail in chapter 3.3.4.

3.2.7 Policy life-cycle

No matter how well-devised Information Security policies are, they must not remain static and need to be subject to regular review and change, not only if there are specific and pressing reasons to do so. Nevertheless, such reasons may be:

- Technological changes in a company’s infrastructure: Due to technological advancements in general or for other technical reasons (e.g. change of an operating system’s platform), a company’s infrastructure may experience changes which may require an update of the current version of Information Security policies. Although the impact of technological changes generally does not have great impact on Information Security policies, because these deal primarily with work processes, e.g. changing a company’s ERP software from one solution to another (e.g. Microsoft Dynamics NAV to SAP or vice versa) will surely have a strong enough overall impact on a company’s work processes to necessitate a revision of its Information Security policies.

- General technological advancements: General advancements in the level of technology that is being used by society can also have an impact on Information Security policies. Faster computers and access to broadband Internet with increasing bandwidth are only two of many reasons why Information Security policies require regular updates to match the ever-advancing and ever-changing environment of potential Information Security threats.

- Changes in legislation: Since Information Security policies are heavily dependent on the current state of law, changes in legislation affecting Information Security often result in an update of Information Security policies. Exceptions to this are cases in which Information Security policies follow a stricter path than actually required by law. This may happen if a company’s management comes to the conclusion that the current state of law on Information Security might not sufficiently protect its

information assets (e.g. documents containing technical know-how about a new prototype or a revolutionary scientific discovery).

- Identification of new threats: New threats against Information Security are developing every day, some of them make it into the media, others do not. Nevertheless, those responsible for Information Security cannot rely solely on the media when it comes to identifying new potential threats for the Information Security of their company. They have to be up-to-date on new technological or sociological developments, identify potential Information Security risks and find ways to counter these threats. As a result of such discoveries, Information Security policies may have to be changed.

  A good example of this is the recent spread of so-called 'social networks' such as Facebook. While these present a sociological phenomenon, they also present Information Security responsibles with a whole new set of problems concerning Information Security: there is simply no way to tell whether employees using Facebook (or any other social networking platform) still handle information assets according to a company's Information Security policies. Another example of this kind is the popular VOIP software 'Skype' that uses a technology called 'UDP punching' to successfully bypass many corporate firewalls. It is not only information assets that may be endangered by the use of such applications, Malware may also be installed through it onto an employee's computer. Recent cases have shown that Facebook users are popular victims for attacks resulting in the insertion of malicious software onto a client's computer. These attacks were based on Social Engineering tactics, motivating users to click on a button that was said to direct them to an interesting video. The destination of such a link was a fake website that was made to look like Facebook in order to fool the user into believing that they were still there, only on another page. Once the users reached that page in hope of viewing the promised video, they got a message that for this video to work they had to update a popular multimedia software called 'Flash player'. Since that message, in the eyes of the users, could have been legitimate, many users agreed to download an installer which in reality contained Malware.

- Consequences of recent Information Security incidents: Part of staying up-to-date with recent developments related to Information Security is to stay alert for recent Information Security incidents. When an Information Security incident took place at some other company, maybe even a competitor, knowledge about this is tremendously valuable because it raises the very important question 'how would we have dealt with this?' Learning from the failure of others without having to pay the price for it is an essential part of responding to such incidents. It offers the opportunity to evaluate a company's defenses against Information Security incidents without actually putting the company in danger. If the result of such an evaluation leads to acknowledging that the current version of Information Security policies would probably have allowed such an incident to happen at one's own company, this clearly dictates an update of these policies.

On the other hand, an Information Security incident that happened within one's company will result in consequences, not only if it resulted in actual damage to the company, but also if the reaction to that incident was not what it should have been. Apart from following normal procedure in case of such an event (classification of the incident, proper response and reporting – steps which need to be clearly defined within Information Security policies), further consequences may be directed at one or more persons involved in the incident (e.g. a repetitive class on Information Security if violations of Information Security policies have been committed by these employees). On the other hand, if the incident happened because the current version of Information Security policies did not sufficiently cover some aspects that were violated during that incident, the necessity for an update of the Information Security policies is clearly evident. The same happens if the follow-up steps of an incident's occurrence (classification, response and reporting) were not performed satisfactorily in order to prevent such failure in the process of Information Security incident handling in the future.

- Change of management priorities: Since a company's view on Information Security is basically top management's view on Information Security, a change in management priorities can have a strong impact on Information Security policies. For reasons that are purely economic, relate to a desired change in the image of the company or even to the replacement of management staff, management may decide to set new priorities for the company. These may include a change in their view on Information Security which entails a change in Information Security policies that can go both ways: for better or worse (from an Information Security point of view).

If none of the above reasons occur, reviews of current Information Security policies should be taken at least every six months to see if they are still up-to-date. In case that such a review or one of the above reasons reveals the need for a change in Information Security policies, the whole company (e.g. all departments) or only specific departments insofar as they are affected by the change have to be informed.

3.2.8 Staying up-to-date on Information Security matters

Besides looking out for recent Information Security incidents, Information Security policies should also specify other responsibilities that have to be taken care of in order to stay up-to-date on Information Security matters. These include keeping apprised of:

- Current technological trends and advances: Advances in technological fields and new trends in information presentation and sharing go along with new possibilities for the handling of information. In order for these possibilities not to become potential threats to a company's information assets, Information Security responsible personnel must stay informed about these trends and the current level of technological advances in the sector of information handling and processing.

- New potential threats to Information Security: Along with keeping up-to-date with current technology and trends, potential Information Security threats should best be

identified before an actual incident takes place somewhere in the industry, maybe even at one's own company. This means that with every new trend or technological advance that can be identified, the question 'could this pose a threat to our information assets?' has to be asked and, if answered in the affirmative, be met with proactive measures.

- New products, software tools and vendor offerings that can support Information Security efforts: In order to support Information Security efforts, new products, tools and offerings by vendors must be taken into consideration. This is not restricted to mere product presentations by vendors, one must also check on benchmarks for these products, look up test reports of their performance and compare them to competing products and tools in order to find the best solutions to support a company's Information Security efforts.

- Upcoming Information Security conferences, meetings, presentations and other events that offer networking possibilities with other experts in the field of Information Security: Attendance of Information Security conferences, meetings, presentations etc. is vital to ensure that one stays in touch with current events in the field. Not only are these events valuable in terms of what they primarily offer (presentations on topics of interest by renowned speakers), but they also offer the chance to network with other Information Security professionals in a relaxed, yet highly productive atmosphere. Some would even go as far as to say coffee breaks and the stimulating conversations that take place there are the most rewarding and valuable part of such an event. This perspective is supported by Harrison Owen who developed this kind of phenomenon into the so-called 'Open Space Technology' which presents professionals of any field of work with the possibility to share each other's knowledge in just such an environment during the course of a meeting with up to 2000 or more participants (see http://www.openspaceworld.org for a presentation of this approach).

- Recent or upcoming Information Security-related publications, literature, media articles: To stay alert for potential Information Security threats, one must continually check for Information Security-related publications, media articles and literature to see if it has any relevance to the Information Security efforts of one's company. The supply of such content to an interested audience is made easy by the use of automated news providing technologies like Twitter, RSS feeds, E-mail newsletters etc. Most well-known online resources (e.g. Bugtraq) offer such services to facilitate the distribution of relevant news and issues of concern among their subscribers. It is an important quality of an Information Security responsible to have a keen eye for such news to stay up-to-date with the world of Information Security.

- State-of-the-art training methods: Training is a major part of Information Security efforts for achieving the necessary level of employee awareness on Information Security issues. As keeping such a level of awareness is essential for any Information Security program to work efficiently, it is imperative to find training methods to keep

it that high without allowing employees to become used to these methods and dismiss them as boring after attending two or three Information Security trainings.

- Current state of law concerning Information Security matters and requirements for security certifications: The importance of the relation between Information Security policies and the current state of law has already been discussed. In order to maintain up-to-date, company-wide Information Security and updated Information Security policies that comply with the relevant laws, any change of legislation (e.g. the European etc.) must result in a critical review of the validity of the current version of Information Security policies. It is therefore imperative to keep up-to-date with the current state of law as well as any requirements for maintaining a security certification (e.g. ISO27001, the Versign Trust Seal or the German 'IT Grundschutz Zertifikat') that a company wishes to hold.

3.3 Components of Information Security policies

One of the reasons why Information Security policies or other written materials concerning Information Security are often inefficient in their implementation is that they lack a clear definition of content placement. In other words, a clear picture of *what* (content) should be put *where* (which document) and *how* (in what detail) has to be present to create effective Information Security policies. Failure to provide such a comprehensive picture may result in Information Security policies which are not only hard to read, but also force too much information on their readers where such detail is not required, while at the same time lacking detail in cases where it is sought by a reader, thus leaving him confused about proper conduct. In such negative cases, the only function that Information Security policies serve is their mere existence for the fulfillment of legal requirements. While in some companies this may be seen as enough, from an Information Security point of view it is clearly an insufficient approach: such policies exist only in theory, and will be ignored by employees due to their complexity and shortcomings in both structure and content placement.

To prevent this from happening Information Security policies need to be clearly structured and well-devised not only in their writing, but also in their content placement. While this thesis' major focus is not on the drafting of Information Security policies, it should be noted that their effectiveness naturally depends on these factors. Consequently, Information Security policies devised in a way that makes them difficult to follow for a company's employees present a challenge for their own successful implementation. In the context of this thesis' main focus – i.e. overcoming challenges in the implementation of Information Security policies – it is therefore reasonable to explore the factors that prevent Information Security policies from becoming such a challenge themselves.

The approach to this goal used in this thesis is mainly, but not solely, based on Mark B. Desman's description of Information Security policies (Desman, 2002 [2001]: 47). This approach defines Information Security policies as consisting of at least the following parts (additional parts may be added if needed):

- Policy statement
- Standard section
- Procedures
- Guidelines
- Classifications
- Definition of terms

3.3.1 Policy statement

The policy statement's purpose is to summarize a company's view on Information Security in simple, concise sentences that leave no doubt as to what needs to be protected (i.e. which information assets need protection) and where responsibilities for this protection lie. It consists of short messages expressed in the form of absolutes, e.g. in case of a statement of least privilege (which should definitively be part of a policy statement):

> "All persons shall have access to all information assets necessary to perform their work functions and none other." (Desman, 2002 [2001]: 48)

Policy statements deliberately show a lack in detail as to their actual implementation in order to make them more applicable as general company statements, forming the base for all further efforts in Information Security. As the policy statement is the highest-level document within Information Security policies, standing above all that derive from it, it is the one statement that is read or referred to the most when it comes to Information Security issues. It is also the one document of Information Security policies that should be distributed as much as possible through all the communication channels of a company to anywhere its presence is required. Its design, wording and meaning have to precisely meet the requirements of simplicity, yet undeniable correctness about the proper handling of information assets, their identity and who is responsible, from top to bottom of a company. By design, it should be very hard for a reader to reject its content.

The policy statement should not exceed (at least not by much) a single page, as everything longer than that will barely be read by employees, which in case of an Information Security policy statement is something to be avoided by all means. Also, as it is the most general document of Information Security policies, jargon of any kind should be avoided to make sure it is as understandable as possible for a general reading audience. This holds especially true for technical jargon as well as legal wordings that might result in complications or misunderstandings on the readers' part.

While all of these criteria make the policy statement understandable and acceptable to a large reading audience, they have an additional advantage: In case of management, the Information Security policy statement presents an overview of the general course that Information Security is taking within a company. Since it is per definition the company's, i.e. its management's view on Information Security, understanding it and agreeing to it is also the basis for any further efforts in Information Security. This fact is crucial in dealing with management when it comes to negotiating the budgets for such efforts: negotiations do not

start from zero if at least the Information Security policy statement has been understood and agreed on by management. It can then be used by an Information Security responsible as a point of both reference and departure for further Information Security efforts to secure a company's information assets.

An Information Security policy statement consists of three parts (Desman, 2002 [2001]: 61):

- The purpose section: Describes the purpose of the document in clear, concise and absolute sentences.

- The scope section: Defines the area that the document covers, i.e. the definition of information assets within or outside of a company.

- The definitions section: Explains each and every term used in the Information Security policies that might not be self-explanatory in order not to leave any room for possible obscurities or misunderstandings.

The following page shows an example taken from Desman (2002 [2001]) that illustrates what an Information Security policy statement may look like. While this specific instance of an Information Security policy statement exemplifies all the factors described above, it must be noted that it is indeed an example for an *Information Security policy statement* only, not – as the document's header would seem to indicate – an Information Security policy in its entirety. Although the section called 'Policy Statement' is just a part of this document, the Information Security policy statement is really not just that section, but the entire document. (Avoiding ambiguity, as we can see from this example, is truly essential to Information Security policies.)

ABC Corporation
Information Security Policy

Purpose

To identify ABC's information resources as corporate assets. To define the responsibilities of those through whose hands these resources pass. To state the corporate position on the handling, use, and disposition of these assets and the provisions for penalty for misuse of said assets.

Scope

This policy incorporates all information assets owned, used, or produced by ABC or its subsidiaries and its provisions cover all persons or organizations who may come into contact with them by means of responsibility, business contact or coincidence.

Definitions

All information resources are hereby defined as ABC corporate assets. Assets are those items that are of monetary value to the corporation. It is stated that no assets – save staff members – are of greater value to the corporation than are the information assets. For purposes of this policy, assets used or produced by ABC are deemed to be owned by ABC.

Principle of Least Privilege

All users of ABC information will be granted access to all of those information assets necessary for the performance of their duties and none beyond that.

Policy Statement

- Any use of ABC information assets must be done in compliance with ABC information security standards and procedures.
- Any use of ABC information assets may be monitored and recorded to ensure compliance with ABC information security standards and procedures.
- Information assets may be used for ABC business only, without exception.
- Access authority or entrusting with assets is granted to the individual and may be used only by that individual.
- All legal, licensing, or contractual requirements involved in the use of assets will be adhered to completely. Copying of licensed software outside of the provisions of that license is strictly forbidden.
- Information or software may be removed from ABC premises only with the authorization of the manager responsible for those assets.
- Failure to comply with the provisions of this Policy or the Information Security Standards and Procedures is grounds for disciplinary actions that may include termination and/or prosecution.

Responsibilities

- ABC senior management is responsible for the implementation and support of this policy
- Line management is responsible to support this policy and to ensure that respective staff members comply with the policy as well as the standards and procedures.
- The manager or information security is responsible for preparing, maintaining and, updating these documents as necessary and for the discovery and implementation of restrictive, measuring, and monitoring measures to ensure compliance with said policies, standards, and procedures.
- Each employee, contractor, vendor, customer, or other party entrusted with access to ABC information assets is responsible for the maintenance of said assets in compliance with this policy, the standards and procedures and other such documentation as management might see fit to implement.

Fig. 2: Example for Information Security policy statement for company ABC (Desman, 2002 [2001]: 61)

3.3.2 Standard section, procedures

The standard section of an Information Security policy describes ways of implementing the absolute statements of an Information Security policy statement. Whereas these short statements document a company's view of Information Security without going into great detail, the standard section describes what has to be done to accomplish this. It is important to realize that while these standards offer additional detail on the implementation of the statements presented in the Information Security policy statement, they do not go so far as to describe how exactly this is to be accomplished. This is left for procedures to specify.

When considering the proper implementation of Information Security, many companies fail to understand the differentiation between policy statement, standard section and procedures when it comes to content placement. As a result, Information Security content gets mixed up between these sections where an exact separation of content and detail according to the purpose of each section should exist in order to make the individual sections meaningful and the Information Security policy effective.

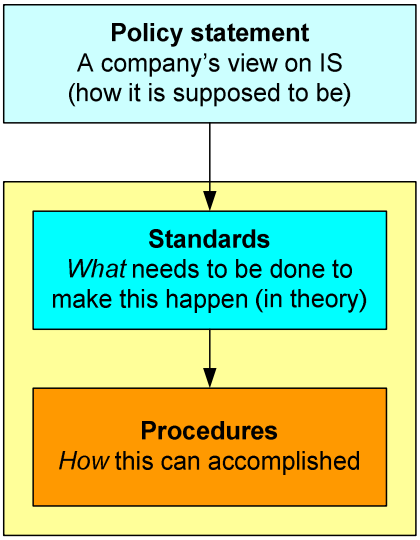

Fig. 3: Classification of policy statement, standards and procedures

As the policy statement is a representation of management's view on Information Security, the standard section should contain all Information Security issues that have been brought up by management during the interview phase that is usually conducted before the creation of Information Security policies. Since the procedures describe the way that standards can be implemented to fulfill them, it makes sense to put standards and procedures not in different documents, but to combine them in a way that first presents a standard and immediately follows it up with the corresponding procedures and only then move on to the next standard.

An example for a standard could be (Desman, 2002 [2001]: 63):

> "Passwords will be changed no less often than every 30 calendar days."

This clear message specifies what needs to be done while leaving no open questions. It could be followed up with the following procedures informing the reader how the aim expressed in the above message can be accomplished:

> "Passwords require at least 8 characters, one number and an upper-case character."

> "No passwords that have been used in the last five password changes may be used as new password."

Additionally, in this context, pointing to a *guideline* about proper password design would make sense (more on guidelines in the following chapter).

In reference to the Information Security policy statement, standards must exist for any relevant topic. Some of these topics could be:

- Protection of information in general
- Log-ins and Log-outs
- Network terminals
- Corporate networks
- Cryptography
- E-mails and E-mail handling
- Internet use
- Remote access
- Software installation and utilization
- Virus protection
- Backup and recovery
- Physical security
- Notebooks, PDAs, Smart phones etc.
- Telephones, Cell phones
- Personal responsibility, awareness
- Violations of policy standards, possible consequences

3.3.3 Guidelines

Guidelines are used to help employees in the process of following procedures to fulfill standards. These documents are on the lowest end of the Information Security policy grading and are also the ones most practically used by employees because of their high level of detail. They contain helpful hints and relevant information so as to help employees fulfill Information Security standards. Good examples for guideline topics are:

- Design of secure passwords
- Proper disposal of sensitive information carriers (manuals, E-mails, CDs/DVDs etc.)
- What to do if a computer becomes infected with a virus

- Physical access and security (entrance to the company building through turnstile using access card)
- What to do if Laptop/PDA/Smart phone/Mobile phone got lost or stolen
- What to do in case of suspected identity theft

While writing guidelines, there are some things to look out for:

- Easy to read, clarity: As with all Information Security policy documents, it is vital that guidelines are easy to understand. Guidelines, however, are different from a policy statement or standards insofar as they are more specialized in one field or area. This may make it necessary to use specific lingo, i.e. specific terms, to describe the content of a guideline. If available, it is always a good idea to have someone from the Documentation department look over guideline drafts to ensure that they fulfill the requirements of readability and clarity while not omitting any necessary details.

- No content that belongs in a document higher in grading: Guidelines are meant to focus on one specific topic only. In the process of writing, however, an inexperienced author may get lost in upper-end theory about the topic he or she is writing about. This not only makes the guideline longer than it is supposed to be, but also fills it with content that does not belong there. While it is acceptable to reaffirm certain relevant points, such repetitions should be kept short. Anything longer should be put into a document higher in the Information Security policy grading (procedure or standard) and be referred to, so as to keep the guideline succinct.

- Finding out what guidelines are needed: Interviewing all departments that may be affected by Information Security measures put in place in a company is a vital part in the preparation for designing and implementing Information Security policies. While this stage in creating Information Security policies serves the acquisition of requirements that an Information Security policy needs to cover, it also brings clarity about which Information Security-related topics need further coverage in the form of guidelines. The complexity of these topics may vary from the simplistic to the challenging, yet this should not make any difference as to the necessity of a guideline written about this topic. It is also important to remain attentive to further demand for new guidelines and provide them as fast as possible if the need arises.

3.3.4 Classifications

Classifications are necessary in order to classify certain information and assign certain operations to these classes that need to take place in case an attempt is made to access this information.

In an Information Security context, at least the following types of information should be classified:

- Confidentiality of information assets

- Access rights
- Incident classification
- Risk levels
- Information system classification

Confidentiality of information assets: In any company, there should exist different levels of confidentiality when it comes to information assets, e.g. public, internal, private and confidential (Mitnick, 2002: 264). All these levels require different procedures in case an attempt to access this information is made. The following table shows an example of what such a classification could look like:

Classification	**Description**	**Operation**
Public	Can be freely released to the public or shared with anyone.	No need for verification.
Internal	For use within the company only.	• Identity of requestor of access to the information must be verified as active employee. or • Nondisclosure agreement on file with management approval for nonemployee must be verified.
Private	Information of a personal nature, intended only for use within the company.	• Identity of requestor of access to the information must be verified as active employee or external requestor with authorization to access private information. • Additional HR department check for disclosure of this private information.
Classified	Shared only with people with an absolute need to know within the company.	• Verify identity and need to know of requestor. • Release only with prior written consent by manager, information owner or designee. • Check for nondisclosure agreement on file. • Only management may disclose this information to nonemployees.

Fig 4: Confidentiality of information assets (based on Mitnick, 2002: 335)

Access rights: With different levels of confidentiality come different levels of access rights to information assets, corresponding to and bound to these levels of confidentiality. The number and nature of these levels or categories of access rights, again, depends highly on the nature of the company that wants to restrict access to information assets by using them. However, not only information assets are affected by access rights; so is physical security in case of accessing server rooms, computer terminals etc. These, too, should be granted only after checking a requestor's access permissions.

Incident classification: In case that Information Security incidents occur, it is necessary to have a plan beforehand which contains steps that have to be taken immediately upon discovery of the incident. The absence of such a plan or failure in its execution can result in the loss of valuable time which often translates to a monetary loss. The reason for such a plan to exist is thus to enable correct and immediate reaction to an Information Security incident in order to minimize such losses.

In order to establish such a plan, potential Information Security incidents need to be categorized, at least broadly, to have a basic idea on how to proceed after their occurrence. Since neither the way Information Security incidents happen, nor their consequences can be fully anticipated, this can only be done in broad terms, so that if something happens, some kind of additional decision making with regard to the response will have to take place in any event. Still, with a plan in place, basic decisions can be automated to leave more time and resources to deal with more complex issues.

The kinds of classification that exist and the steps that have to be taken in case of an incident can vary greatly depending on the nature of a company. The only certain and definite dependence of an incident classification regards the level of confidentiality of the information involved in the incident. In other words, if an incident involves, e.g. the loss of classified information, this will most likely result in a classification of this incident with the highest available incident classifications.

Risk levels: Classifying the risks of Information Security incident occurrences is an important aspect of Information Security incident management. This means that after the identification and classification of potential incidents, the company in question needs to evaluate the costs for measures to prevent such an incident and define the risk it is willing to take of this incident actually occurring. Naturally, incidents with a potentially graver impact on a company will be met with a lower willingness to risk their occurrence by that company. This leads to different levels of risk that need to be identified in order to assign them to potential incidents in the future.

Information system classification: The handling of sensitive information involves processing this information using different kinds of information systems. The nature and sensitivity of these systems depends on the nature of the information that is being handled through them. Based on this relation, a classification of information systems is required to determine their level of criticalness, i.e. the impact that a temporary (or permanent) malfunction or disruption

of a particular system will likely have on current operations (e.g. as a result of a denial of service attack).

3.3.5 Definition of terms

Human communication is prone to misunderstandings. Different cultures, languages, attitudes and approaches to problems lead people to different conclusions in the evaluation of situations they find themselves in. Especially in cross-country business relations, this can be difficult if measures to reduce possible misunderstandings are not taken in advance.

One common source for such misunderstandings can be avoided by assuring that when information is communicated, employees at the receiving side understand the terminology used in such communication in exactly the same way as intended by the sending side. This can be achieved by simply maintaining a list or glossary of terms that are used in a certain field of operation the company works in and making sure that each employee familiarizes him- or herself with these terms with the help of that list. This list has, of course, to be updated with new terms that might come up in the process of operations.

While it stands to reason that some terminology can be assumed to be well-known to anyone operating in a certain field of work, it is better to be on the safe side and have a comprehensive list of terminology to be used throughout the company, not solely when it comes to Information Security, but anywhere and anytime. Doing so assures that, over time, people become accustomed to that terminology and begin using it themselves when communicating in work processes, thereby reducing the chance of misunderstandings based on a different use or understanding of terminology.

4. Challenges in establishing Information Security policies

The process of establishing Information Security policies can be a challenging experience not only for members of the responsible Information Security department, but also for all other employees who come into contact with Information Security measures that are put into place in the course of such an implementation. However, even before the implementation phase, the creation of Information Security requires certain advance preparations in many different areas in order to allow a smooth transition into a more secure state for a company handling information assets. These preparations are necessarily based on already existing knowledge about some of the most common challenges one has to face in the process of implementing Information Security within a company. The nature of these challenges is very broad and seldom involves purely technical issues which might be addressed with a technical solution, but also more employee-related issues which are not as easily resolved. Although sophisticated technical solutions to counter these issues may exist, they cannot solve them on their own, but merely provide support in the larger efforts to do so. Bruce Schneier, in his book 'Secrets and Lies', stated that "It's clear to me that computer security is not a problem that technology can solve. Security solutions have a technological component, but security is fundamentally a people problem" (Schneier (2000): xii). Although this quote refers more generally to Computer Security, its conclusions can be extended to Information Security as well.

This chapter presents some of the issues and challenges that might come up in the process of creating and implementing Information Security policies within a company. While in some occasions, directly applicable solutions to these problems can be presented, the majority of the following challenges are of a more complex nature. This thesis will therefore first present these challenges, note their existence and explain what they consist of, while the subsequent chapter 5 presents an applicable approach, explaining how they can be overcome.

4.1 Finding allies

No matter what field security professionals operate in, one challenge they are constantly faced with is the fact that the measures they put in place to protect company assets affect the whole company, i.e. an often much larger group of people in departments that are very different from their own. In a small company, that may not present much of a challenge, but in larger companies it may very well, depending also on the field of security in question. While a network security professional, for instance, who has complete control over a company's gateway to the Internet, can easily enable or disable access restrictions for the whole company by establishing corresponding firewall rules, such technical means of control are not available to Information Security professionals in their field of responsibilities. Indeed, professionals in probably no other security field are more dependent on user compliance than in Information Security, because monitoring each and every user is impossible out of the sheer majority of users versus a relatively small number of Information Security responsible personnel. Besides this problem in numbers, this dependence on user cooperation presents another challenge that

every security professional has to deal with: Since security measures go hand in hand with constricting people's accustomed ways of going about their work (which they normally do), the affected people's initial reaction is most often one of resistance or, worse, an attitude of 'them against us' contra the responsible security department. It is then seen as a disabler, making their work more difficult than it already is, instead of an enabler who has something of value (security) to contribute to their work.

Clearly such an attitude adopted by employees can make the job of an Information Security responsible very hard. Since Information Security responsibles find themselves in that dilemma (constricting people's lives while trying not to provoke such a response to their work and department), they have to find ways to present themselves as enablers, not disablers. This is vital to having a chance of successfully meeting their responsibilities, because without such a position within a company (i.e. compliance by the employees affected by Information Security measures put in place), no Information Security policies, no matter how well devised, have any chance of being implemented successfully because they go against the people whose assets they are meant to protect.

Besides being outnumbered, another challenge that Information Security departments usually face, especially in their initial efforts to bring Information Security to a company, is the budget for the implementation of necessary measures. In many cases, Information Security is a topic that suffers from a lack of recognition by upper management. Consequently, budgets for Information Security measures are limited, often leaving an already under-staffed Information Security department without the necessary resources and funding to give an Information Security professional's vision for a company's Information Security a chance of being realized. While this presents a notable challenge by itself, there are certain persons who can come to one's aid when it comes to budgetary negotiations with management. These people have influence on managerial decisions and are referred to as 'hidden opinion leaders' in this thesis (a detailed explanation of this term and its relevance to Security budgets follows in chapter 4.4). Their support as allies is vital if one is to succeed in getting the required budget to implement necessary Information Security measures. Also, hidden opinion leaders that are not won over as allies may well become obstacles and as such are very hard to overcome.

Because Information Security affects so many different areas in a company, the aid of a number of other departments is of outmost importance because their support, services and channels of information distribution allow Information Security content to be brought where it is needed – to the people that are affected by it and whose information needs protection. These departments usually (but not exclusively) include the following, depending on the size of the company:

- Human resources (HR)
- Information Systems
- Records retention
- Public relations (PR)

- Documentation department
- Internal audit
- Legal and Compliance department
- Application development
- User Management and User Support
- Operations
- Corporate security
- Facilities
- Graphic Arts department

While each of these departments specializes in another field of work, getting to know what department controls which resources and finding ways to get these departments' support is something that Information Security professionals need to dedicate themselves to.

Joining efforts to get Information Security content to the whole company through all available channels should be a major goal for any Information Security professional within a company. Networking of that kind and maintaining good relationships with these other departments while letting them do what they do best in the name of Information Security is a very efficient way to achieve that.

Probably the most important ally that the Information Security department needs for Information Security to work is the 'common employee', i.e. each and every person working in or for a company (this includes external employees or contractors). Without his or her awareness in matters concerning Information Security as well as his or her compliance with the measures put into place by the Information Security department to fulfill the Information Security policy, no Information Security effort will be successful in the long run. Evidently, this does not stop at the company's physical border, but also includes external employees, contractors and business partners. Depending on the size of the company and its field of operation, Information Security policies must not only take into account the range that needs to be addressed, but Information Security professionals also have to find ways to 'win the crowd' (e.g. all persons affected by Information Security) for their ideas or at least gain their acceptance and cooperation in the implementation process. Ideally, in an Information Security sense, employees should, while going about their work, do so while serving as the eyes and ears of the Information Security department. This implies that they are aware of Information Security-related topics that affect their work and, in case of potential danger, act accordingly because they have understood the necessity of Information Security and what it is trying to accomplish. This is what is referred to as 'user awareness' in the context of Information Security and is *the* most important factor determining the failure or success in the implementation of Information Security policies.

One occasionally forgotten, yet valuable ally is one's predecessor with regard to Information Security efforts that have been implemented in the past or have failed to reach or complete successfully the phase of implementation. While this person (or persons, as there may be

more) may not have held the same position as one may be holding now, valuable information can be obtained from him or her about the following topics:

- Previous attempts to implement Information Security
  - Why have they failed or succeeded?
  - What were the difficulties, what came easy?
  - Who else was involved?
  - Where can documentation be found?

- Projects that never made it to implementation, yet addressed a valid issue and deserve to be revived
  - Why was the project never finished? Was the budget not sufficient?
  - Were there opposing hidden opinion leaders or managers? If so, who? Are they still in the company? What were their arguments against the project?

- Would they be willing to help in future projects?

Having such an ally is of great benefit, because one can avoid running into obstacles during Information Security projects that have been encountered before or at least prepare against facing them in advance.

4.2 Knowing the addressees of Information Security messages

It has already been mentioned that in many cases the general attitude of employees towards Information Security is unfortunately one of resistance. Depending on the nature of that resistance and its gravity in the context of Information Security measures, a worst case scenario would allow it to render an Information Security program ineffective, practically useless. Additionally, it can irreparably damage the relationship between employees and the Information Security department along the way, which makes it all the more important to never allow an attitude of ‘them against us’ to evolve on the part of employees or even be reciprocated by one’s own Information Security department. The image that employees have of Information Security and the responsible department is crucial and should be one of colleagues, not enemies or ‘big brothers’ watching over one’s shoulder.

In order to counter such resistance or, even better, avoid it altogether, it is imperative to identify the reasons for which employees react in such a manner when it comes to Information Security issues. While some of these reasons may be more obvious than others (Information Security admittedly makes established work processes more complicated, no one will argue about that point when it is brought up in a discussion about the necessity of Information Security measures), creators of Information Security policies need to identify the reasons that drive employees in their company and field of operation to react the way they do. This applies for both, positive and negative reactions. Knowing the addressees of Information Security policies, who they are, where they are coming from (not literally, of course, but in a context of Information Security), how they have reached their points of view on Information

Security – in short, seeing the company through their eyes is therefore key in gaining their much needed support and, if not make them allies in the cause of Information Security (which of course would be preferable), at least not let them become opponents or even saboteurs of one's Information Security efforts.

4.3 Resistance against Information Security

In analyzing the reasons for a company's employees' resistance against Information Security measures, one or more of the following factors will likely be found in all of them:

- It is in the nature of many people to resist change, especially if it affects well-established processes or ways of thinking.
- People will usually go for the easiest solution to a problem.
- People will usually go for the way that promises their work to be done in as short a period as possible.
- Especially if put under stress (e.g. because of an upcoming deadline) people will bypass security measures (which includes Information Security) in order to get their work done.
- People will only willingly accept burden if they can see a greater benefit in doing so.

All of these factors can often be traced back to insufficient communication by the Information Security department concerning the effects that Information Security has on people's work processes and the benefits it brings by protecting a company's information assets. If people do not understand these benefits, they have almost no choice but to see Information Security as the one thing that is all too obvious to them – as something that makes their lives more complicated than they were before. An attitude of resistance against Information Security under such circumstances is therefore quite natural and to a certain point even understandable.

The early-on identification of resistance factors against Information Security is therefore a necessary measure during the implementation of Information Security policies. Many of these factors depend highly on the company's size, field of operation or even individual preferences. Some are discussed in the following subsections, but it is important to keep in mind that these are just common examples of resistance one may encounter while implementing Information Security policies in the majority of companies of any size. The bigger the company and the broader its field of operation, the more different types of potential resistances one may encounter.

4.3.1 Lack of interest in Information Security

A lack of interest is not a problem that only Information Security has to deal with, but rather a problem of security in general, regardless of the specific security field. Although regular media reports about recent security incidents have brought more and more public attention to

security issues, also raising the awareness of private individuals, security is still something that most people would not care about as much as they should.
It comes as no surprise, therefore, that when confronted with the topic, people's attentiveness and awareness is less than it should be. Measures such as Orientation days classes, obligatory signing of Information Security agreements by new employees before they get access to information assets etc. can do their part in a business context, but the overall attitude concerning security as a topic of little interest remains the same if no further actions to improve it are taken by an Information Security department.

The challenge that presents itself is to make security – and, in the context of this thesis, especially Information Security – a topic of interest or at least of enough interest to a company's employees to give it a sufficient part of their overall attention. For this to happen, Information Security must create a personal relation between the topic of the message that is communicated (Information Security) and the recipient of that message (the employees). In other words, it must mean something to them so that it cannot be easily dismissed – whether because of a lack of interest in Information Security or any inconvenience that accompanies it.

Generally, the motivation for someone to do or leave something be is influenced mainly by two factors:

- The fear of losing something.
- The perspective of gaining something.

In case of the challenge in question, this means that people regarding security as a topic of little interest are neither aware of the loss they or their company might suffer in case of an Information Security incident, nor are they aware of the benefits in case that Information Security within a company becomes as strong as it should be. Knowing this, an Information Security department creating an Information Security policy can devise ways of specifically appealing to the two above-mentioned drives for motivation in order to raise interest in the topic of Information Security.

4.3.2 Getting work done as quickly as possible

While Information Security no doubt has its reasons for existence, this comes at a price. As has already been pointed out, in many cases it is an unavoidable side-effect of Information Security that work processes become more complex and time-consuming. Filling out forms to get access privileges to a system that requires patching, going through a specific process chain in order to get approval for a much-needed firewall exception rule – complications such as these can make Information Security a ready candidate for skipping in order to get a job done as quickly as possible.

Nobody wants to work longer on a project than is absolutely required. A problem with this attitude, however understandable it may appear, is the ambiguity of the phrase 'absolutely required'. Many would understand it in a way that interprets Information Security as an *addition* to the original work process that can be skipped if and when it becomes a problem

for some reason. This view of Information Security, however, is a problem by itself, as Information Security has to be seen not as an addition to any process, but as a non-optional, obligatory part that cannot be separated from any process that includes the handling of sensitive information assets. In order for it to work, the nature of Information Security and its resulting inseparability from any process must be successfully communicated to employees.

4.3.3 In times of stress, security gets dropped first

This factor is similar to the one discussed before. Whenever a project pushes employees hard, they will be looking for ways to decrease the level of stress they experience. Depending on that level, one of the first ways of doing so that comes to the mind of many employees is usually bypassing Information Security in order to accelerate the project's progress, e.g. to meet an impending deadline. The problem that underlies this common scenario is again the attitude towards Information Security as something that can be dropped if it becomes too inconvenient, instead of accepting its necessity as an integral part of any process.

An example for this is the famous 'Security vs. Availability' tradeoff. This is probably the most obvious challenge faced by all professionals in their corresponding fields of security. While in theory the advantages of having Information Security may become acceptable to employees at some point, the price they have to pay for these advantages in terms of limitations or complications in availability may remain unacceptable to them if put to the test. A good example for this caveat, although taken from the field of network security rather than Information Security, is the issue of personal firewalls. While most likely nobody would deny their usefulness in protecting a computer workstation from unwanted outside connections (and, if a good product was chosen, also from unwanted inside connections to the outside) and keeping an overview of the network traffic relayed through that particular computer, people tend to change their minds about that as soon as they encounter any kind of network problems on their computer (e.g. no access to network shared directories). If those problems are not solved immediately, the consequence is almost always a deactivation of the personal firewall, thereby 'solving' the problem and enabling the desired access. However, this 'solution' comes with a heavy price in terms of security, which in this scenario has simply been deactivated instead of looking closer for a solution that, in this particular case, would have been a matter of simply defining a corresponding firewall exception rule, thereby enabling availability without abandoning security.

4.3.4 Attitudinal-based resistance

In some cases, implementing Information Security was met with resistance because, out of attitudinal differences, it felt uncomfortable or unnatural to employees to comply with a company's Information Security policy. These differences may have been shaped, e.g. by a different corporate or department culture in which the employee used to work before he started to work at one's company or a new department.

Although a company should obviously respect each employee's personality, in case of Information Security it is clearly the employee who must adapt and follow the Information

Security policy, because he or she has signed a corresponding agreement to do so during Orientation days.

Nevertheless, as someone responsible for the implementation of the Information Security policy within a company, one should always be aware of attitudinal differences as a potential obstacle to employee's compliance with Information Security.

4.3.5 Privacy concerns

Sometimes employees feel that security measures go too far in terms of invading their privacy. Such perception, whether legitimate or not, can lead employees to resist security altogether or just in certain scenarios where they feel that their personal space and privacy is being invaded by their company's desire for security. This is a highly delicate matter, as people's views on privacy need to be respected, yet on the other hand the security of a company must not be endangered.

The best way to deal with this challenge is to provide education about the necessity of security while also communicating, in more ways than just verbally, trust in the employees, and that their privacies are being respected by their company. In almost any case a compromise between those two subjects should be reachable.

4.4 Getting the budget for Information Security

On a number of occasions in this thesis, the topic of obtaining budget has been brought up. Its relevance in the context of challenges in implementing Information Security policies stems mostly from the fact that, unfortunately, Information Security (or security in general) is not always accepted as one of management's top priorities for a company. As a result, the budget spent on Information Security is usually much less than what would be required to staff a company's Information Security department with sufficient employees and bring a company's Information Security to an acceptable level. Also, bringing everyone involved to acknowledge that Information Security is not a one-time investment, but an ongoing process and commitment, is something that can take considerable effort during discussions for budgetary support.

This makes negotiations with management over Information Security budgets a challenging task which should be well prepared for so as to present the best arguments for obtaining a budget while also having the support of 'hidden opinion leaders' and other relevant contributors to one's cause. (This thesis uses the term 'hidden opinion leaders' to denote people who have significant influence on the decisions made by management. Through extensive know-how and competence in their field, these employees have a level of expertise that has made them management's choice when it comes to obtaining a reliable opinion on something in their field of work and deciding whether further budget is to be granted or not. Winning them as allies and gaining their support is therefore crucial for debates with management over budget issues.)

When preparing for these discussions, one has to realize that budget negotiations for Information Security projects are no different than for any other project that requires budgetary funding. In the end it is about convincing upper management of the importance of the project, presenting the benefits it would bring to the company, the losses it could cause the company if it was not undertaken and, last, the budget that is required to do so.

In the process of preparing for such a task, one may encounter some of the challenges discussed below.

4.4.1 Finding allies for budget negotiations

This topic, for the most part, has already been discussed in chapter 4.1. In the present section, the focus lies on determining who these allies are that one should be looking for in order to get their support for budget negotiations.

Hidden opinion leaders: Winning them as allies to support one's position on an Information Security project is obviously vital to winning an argument over getting it started and being granted the necessary budget. Locating them within a company can be difficult, as they are often inconspicuous employees. Their status as opinion leaders remains relatively hidden to outsiders and is known only to colleagues of the same department and the managers who seek their expert opinion on matters in their field of expertise. The only way to discover if a hidden opinion leader exists in one specific area or department (which evidently would be affected by the Information Security project in question) is by interviewing employees that work there.

Middle management of affected departments: By design, Information Security affects many departments within a company and may likely also address some of the issues that have been identified within these departments. If these issues have already been identified and labeled as such by the respective departments' managers, it should not be difficult to gain their support in providing help with a solution that not only addresses them, but is also in the interest of Information Security. Finding common ground for such a solution that serves a dual purpose is thus one way to gain the support of the managers of these departments, especially if the issues addressed are open audit issues that have been found in the last internal or external audit. Depending on the classification of these issues, pressure on fixing them may be high as they probably have been reported directly to upper management in the corresponding audit reports.

Predecessors: As has been discussed in chapter 4.1, looking up one's predecessor (whether in general or only in relation to particular project) and gaining his or her support (if he or she is still employed by the company) for a particular Information Security project can be very valuable. Previous holders of this function should, whenever possible and reasonable, be kept active as consultants to the current holder of that function. Whether they should act primarily as a mere source of information or also as highly visibly members of the Information Security team will largely depend on the person's standing inside the organization.

Internal auditors: The relationship between internal auditors and the rest of a company (including the Information Security department, which can also become subject to audit) can be adversely affected for similar reasons as with other departments. However, the recognition that internal auditors are also identifiers of potential Information Security risks makes them not only allies, but also support candidates for budget negotiations with management. It is therefore imperative for the Information Security department to establish and maintain a good relationship with the internal audit department and openly communicate the shared interest of a higher level of Information Security for the company (which is certainly one of the auditors' concerns as well) as well as the willingness to help with reaching that goal. One great benefit of such a positive relationship is that internal audit reports are normally given a high priority by upper management. If therefore the Information Security project in question happens to address open audit issues that are known to upper management because they have been put in the last audit's report, this kind of support of one's project is invaluable in discussing the funding of this project with upper management.

External auditors: Everything that was said for internal auditors equally applies to external auditors as well. The difference between these relationships is that external auditors are harder to reach, because they are not part of the company and only visit it while performing the audit and present their findings afterwards. However, since external auditors audit, among other things, the legal compliance of a company's efforts with the current state of law, their reports can go up to the highest level of management. Having open audit issues and recommendations in these reports to which one's project presents a solution is therefore as good a support as one can ask for when discussing such a project's budget with upper management.

The establishment and maintenance of such a relation with external auditors is not as hard as one might expect. As external auditors seldom expect much cooperation from the employees of the companies they audit, giving them full and extensive cooperation while also making suggestions in the direction of the problems to be addressed by one's own project, can result in the incorporation of these suggestions into an external auditor's end report and consequently on the desks of upper management.

Direct superiors: Not only because of his or her relation standing as a superior to one's position within a company, but even more so because of the ways a superior can help one reach any of the potential allies mentioned above, the support of a direct superior is required for almost any project. Additionally, he or she may have experience in budget negotiations with the managers responsible and may provide valuable insight into what to expect, what to prepare for, and what to focus on while presenting the case for one's Information Security project. Including a direct superior in a project's planning and sharing concerns about financing that project is therefore strictly in the interest of realizing such a project.

4.4.2 Finding exemplary Information Security incidents

Good arguments for security can always be found in the form of real incidents that could have been prevented by measures that one is currently trying to get a budget for. The best way to present such an argument is to take an exemplary incident, best one that took place at some

other company, create an imaginary scenario in which a similar incident would have taken place in one's own company and ask the question 'how would we have reacted?'. After preparing one's own response to this crucial question, the same question is put to the management responsible for budget allocation. While at the same time presenting an answer that is not satisfactory in terms of Information Security, indicating that one's own company would, under the current circumstances (i.e. without what the proposed project would accomplish), have suffered a similar fate as the other company, this should strengthen one's argument for the necessity of a project to counter such an incident. By implication, that means that financing such a budget is not only in the company's interest, but a necessity.

The problem with this approach lies in getting the necessary details about such an incident. Only a few of such incidents become known to the public, while the majority remains in the dark. The reason for this is that companies suffering from such incidents have no interest in suffering a bad reputation, becoming ridiculed in public for their lack of preparation for such an event or, even worse, costumers losing faith in them and turning to a competitor instead. Also, depending on the dimension of the damage caused such an event can cause investors to lose interest in the company, resulting in a stock market loss. Getting information to support one's cause (the approval for budget for an Information Security project) which someone else is actively trying to hide is not an easy task, especially since there are some very comprehensible arguments for the management of companies that have become victims for not wanting to share such information as:

- The number of costumers lost shortly after the incident (provided it can be assumed that this loss was a direct consequence of the incident occurring)
- The quantity of stock market loss
- The quantity of monetary losses
- A loss of contracts because of the damage to a company's reputation
- A negative public image (e.g. the recent case of Google being accused of sniffing traffic from private, open Wifi networks) or loss of reputation

Again, getting any details on these facts (while not humiliating anyone) may prove difficult, but worthwhile the effort of researching if they can later be presented to management as further proof for the necessity of an Information Security project that would prevent similar incidents from happening to one's own company.

Of course, if such an incident has taken place at one's own company, this presents an even greater possibility for increasing Information Security, because the current level of Information Security was obviously not sufficient to prevent it. Getting supportive data on such an incident should not, since it has occurred at one's own company, prove too difficult. The only sensitive issue to avoid in this process is to point fingers or blame colleagues (for obvious reasons), but to stay focused on the need for further Information Security efforts in order to prevent such an incident from happening again. Also, if the incident happened because of the absence of Information Security measures whose implementation one already proposed some time ago, but was refused by management, this lends additional support to one's cause.

4.4.3 Getting success stories – the security dilemma

Information Security incidents at other companies can support one's request for budget for an Information Security project as has been described above. On the other hand, *success* stories that convey the positive outcome of incidents at one's own company because of Information Security measures that have been put in place provide backup for these measures, while also raising confidence in one's abilities to protect a company's information assets.

The problem that needs to be faced here, however, is a dilemma that is shared by all security professionals, regardless of the area they operate in:

> Success in terms of security is defined by the absence of security incidents.

This basically means that if nothing has happened at a company that threatens Information Security, this can be interpreted as evidence of Information Security working as it is supposed to. However, feeding 'nothing', even in this context, to management as an argument for further development of Information Security efforts within a company will most likely prove to be insufficient for getting a budget for these efforts approved.

In light of this dilemma and the problem it causes in negotiations over additional Information Security budget, it becomes increasingly important to constantly collect data that indicates that the Information Security measures that have been implemented so far have indeed been successful (if they were) and are thus worth the money and efforts invested in them and present them as the main reason why nothing bad has happened so far. (Details on what this data is and how to best present it to management in budget negotiations will be discussed in chapter 5.6.6.)

With such data at hand, it is easy for management to see that the budget spent so far has been used effectively to protect the company's valuable information assets. Together with reports about recent Information Security incidents that occurred at other companies, this should support one's position in getting a budget for a particular Information Security project that further enhances the protection of these assets.

4.4.4 Making Information Security a management top priority

Information Security is an ongoing and developing process that requires constant attention, improving and dynamically adapting to all kinds of new, upcoming threats to a company's information assets. In order to ensure sufficient budget to maintain and consistently update this process, sensibilization of upper management to this fact should make it a top priority for a company and its management. Getting to that point requires convincing management about the following subjects:

- The value of information
- Knowledge about the existence of information assets and what kind of information they contain (content, confidentiality etc.); not in detail, of course, but more generally

- Potential threats against information assets
- Risks of incidents occurring
- Acceptance of Information Security being a process, not a one-time product that can be simply bought, implemented and then forgotten about in a false feeling of security.
- Knowledge about Information Security approaches being proactive, not reactive and that the absence of Information Security incidents means that these approaches have most likely been implemented successfully.
- Acceptance of Information Security not being a technical issue, but primarily a challenge based on people's behaviors, requiring adequate measures to deal with it.
- People's general attitude and response towards security
- General security-relevant topics such as the principle of least privilege or the tradeoff between security and availability
- Awareness that Information Security does not stop at a company's borders if it operates cross-country wide, but must also be followed by a company's business partners, at least on an acceptable level.

Getting management to recognize all these points is the basis for getting top-down support for the ongoing process that is Information Security. Also, as the Information Security policy statement has been created with help of and signed by management with full understanding of the above points, this represents the necessary groundwork for any further negotiations with management on the topic of Information Security, whether the topic is budget or anything else related to Information Security.

4.4.5 Getting approval by Finance and Controlling

With the above taken care of, it remains to actually acquire the budget needed to implement certain Information Security measures. While finding allies and exemplary incidents as well as presenting success stories has (hopefully) allowed management to recognize Information Security as a top priority for the company, the approval for the actual allocation of budget must pass through the Finance and Controlling department.

The question whether this allocation is to take place is therefore a question of corresponding financial policies of this department which, as a consequence, is also responsible for answering any audit questions concerning this allocation.

4.5 Letting people recognize the value of Information Security to the company and themselves

Chapter 4.3 covered some of the most apparent reasons for employees' tendency to resist Information Security. The basis for all of these is the fact that without any education on the subject, most people will perceive Information Security as something that constricts work processes (i.e. a disabler) instead of something that can actually help them function better (i.e. an enabler), which in the context of Information Security means more secure. The challenge

that presents itself is therefore how to communicate to people that Information Security may indeed make their work processes more complicated than they would be, but that this is a small price to pay for what is gained on the other hand, i.e. that people and the company they work for are better off with Information Security than without it.

For people to see Information Security in such a light, i.e. as an enabler rather than as a disabler, they need to a) know the people that are trying to convince them as colleagues, i.e. familiar faces, not as an obscure department they have heard of from time to time and whose only goal seems to be to make their life more complicated, b) recognize the value of Information Security for them personally and, in the bigger picture, for the whole company. Getting there is, as Information Security in general, mostly a sales matter. While the process of convincing management of the importance of a specific Information Security project in order to get sufficient budget, is basically a matter of 'selling' this idea to them, the same is true of convincing employees. The only difference between those two sales targets is that, while the point of selling something to management from their perspective lies in obtaining something of greater value for the company, employees' attitude towards Information Security is mostly motivated by personal reasons ("what's in it for me?") rather than corporate ones. All the more importance should therefore be attributed to getting to know employees and their work processes in order to understand how to communicate Information Security to them as something that brings value, not just cost, to their daily work.

It is a valid assumption that people who are affected by Information Security do not posses a sufficiently developed technical and/or security background to understand in all detail the importance of security in their company or, in other words, to understand the ways in which even seemingly innocuous information may be used to damage a company. In fact, most of them do not have such a background, yet when it comes to Information Security, this should present no handicap in communicating to them the value of information in a way that is understandable to them, as well as that the information assets they handle on a daily basis should be dealt with on an appropriate level of Information Security. The presence of such *employee awareness* needs to be enforced by any means at one's disposal as this is the most important issue of all when it comes to Information Security.

4.6 Creating and maintaining continuous awareness

The biggest challenge in implementing Information Security policies is the creation and maintenance of a sufficiently high level of employee awareness regarding Information Security. Only then can employees serve as independent allies for the Information Security department, keeping their eyes and ears open for potential dangers and act accordingly if they encounter one. In a nutshell, this is what Information Security is all about. While specific ways to create and maintain such employee awareness will be the topic of chapter 5.5, the following factors are also relevant in creating such continuous awareness on the part of the employees of a company.

4.6.1 Sense of responsibility

Appropriate behavior in the context of Information Security is always the result of people's awareness of the value of information and a sense of responsibility for the information assets that carry that information. Creating such a sense of responsibility is therefore very desirable to a company's management, not only because it can be assumed that an employee feeling responsible for a company's assets (in this case information assets) also carries a certain feeling of loyalty to the company. Such a feeling can be based on a company's efforts to make its employees feel as part of the company collective, sharing responsibilities for all of its assets.

A sense of responsibility for information assets is usually based on each employee's understanding that for Information Security to work, everybody, from top to bottom of a company, has to do their part. This highlights the importance of getting top-down support for Information Security by management serving as a role-model for every employee in the company in terms of comprehension and compliance with Information Security measures.

4.6.2 Consequences of Information Security failure

Part of understanding one's responsibility within a company in terms of Information Security is to know the consequences of failure. Given that the value of information is present and known to the employees (as it should be), it becomes clear that a loss of information equals a loss of money, both to a company and to its employees, especially in case of a shareholding offer held by employees.

Also, employees have to keep in mind that Information Security failure can, in drastic cases, result in disciplinary action or legal prosecution. Typically, all employees of a company have signed an Information Security agreement on their first day at work or during the company's Orientation days. This agreement contains their statement to uphold Information Security as well as their confirmation of having understood that a violation of this agreement could result in consequences including disciplinary action or legal prosecution. Depending on the gravity of an Information Security incident, responsibilities for the information assets in question and the nature of the violation of the Information Security policies, consequences for employees may very well involve discharging an employee or even pursuing legal charges against him or her.

While especially the latter should not be seen as a primary way of motivating employees to adhere to Information Security policies, it should not be forgotten by any employee that Information Security violations can have very unpleasant consequences for him or her.

4.6.3 Diminishment of awareness

No matter how well designed an Information Security program may be with respect to raising employee awareness, over time this awareness will decrease if no countermeasures are taken. The problem that presents itself here is that people become accustomed to the work processes

they operate in on a day-to-day basis, consequently leading to a decrease of awareness. While the creation of the necessary employee awareness is a challenge that has already been discussed, maintaining that awareness so that it remains on a sufficient level and does not endanger the Information Security process requires an approach by itself. Chapter 5 provides more insight into such an approach, some of the challenges one may encounter in creating and maintaining a high level of user awareness, and ways to counter its decrease over time.

4.6.4 Training approach and methodology

An essential part in creating and maintaining awareness is proper training. The challenges that lie herein are:

- Know-how and didactic skills: Obviously, someone charged with providing training in a subject such as Information Security should have extensive knowledge about it. However, knowledge alone does not qualify for training, as knowing about Information Security and being able to communicate that knowledge understandably to an audience are two different qualities entirely. The challenge therefore lies in finding a trainer who not only knows the subject but also knows how to communicate it to an audience – not only in the form of monologues, but using other methods and devising corresponding, usable training materials. This person could be someone from the Information Security department, assuming he or she possesses the required didactic skills, in which case the documentation department could assist in the creation of proper training materials. Alternatively, an external trainer can be entrusted with training, in which case he or she must obviously keep close contact with the Information Security department to ensure that the content being trained is in full accordance with the company's own Information Security department.

  This offers both an advantage and a disadvantage: In some cases, people react more positively to an external professional trainer, increasing the likelihood that the training success will be as expected and intended. On the other hand, hiring someone from the outside denies an Information Security professional from inside the company the chance to gain the status and respect he requires from his colleagues by directly training them and presenting himself as an expert on the subject of Information Security.

- Choosing the proper essentials: Every training session requires choosing parts of the topic being taught that are the most essential to form a bottom line. This bottom line should be easily understandable and should become clear in all training sessions and materials repeatedly in order to stay with the audience. The choice of these essentials depends on the design of the training and the audience that is being taught. Generally, however, there should not be more than a few bottom lines to each training session so that people will remember them more easily.

- Knowing the target audience: No two audiences are alike, it pays to identify some differences in their backgrounds and know-how. Also, any possible presumptions

about the content that is being taught should be taken into consideration. If an external trainer is charged with training, he or she must be briefed on all the relevant information about the audience to be trained, best by an internal Information Security expert (who should know about these things).

- Training methods: Finding the right training methods for reaching the largest percentage of an audience depends on the trainer's style of training and personal preferences, the audience, the subject being taught and the budget for the training. Most important in choosing the right training methods is the differentiation between the creation of awareness and its maintenance. Especially external trainers need to understand the importance of the latter in the context of Information Security (which they should anyway, if they have a security background of some sort).

4.7 Establishing Information Security as an ongoing process

4.7.1 Proactive and reactive approaches

Information Security is, by design, an ongoing process and therefore needs to be established and maintained as such. There are different parts to achieving that, yet all have one thing in common: They are designed to be proactive rather than reactive.

In security in general, any kind of operation can be differentiated into proactive and reactive. Since avoiding an Information Security incident is obviously preferable to damage control, taking the initiative is usually preferable. However, since in security a 100% sure forecasts can not realistically be made, proper incident management, in case something does happen, following a reactive approach is also very important.

Both approaches, proactive and reactive, can be found in Information Security. Information Security itself is mainly proactive, trying to create and maintain awareness of the value of information, the information assets that exist within a company, and the dangers to these assets. By doing so, Information Security tries to *avoid* unwanted exposure of valuable information, marking it clearly as proactive. However, no Information Security policy or program has ever been perfectly designed or executed, incidents are sure to happen sometime, so it is imperative to have proper management steps ready for such a case. This is what is called 'incident management' and is, since the incident *has already* (and unfortunately, if proactive measures have been implemented, but have failed) *taken place*, reactive.

Well-designed Information Security policies enforce Information Security as an ongoing process that consists of combined proactive and reactive operations. The Information Security process itself is proactive while, in case of an incident, proper incident management procedures take place that not only try to limit the damage that is caused by the incident, but also present feedback on the current state of the Information Security process and its proactive components. This is especially relevant for these components that require improvement so that similar incidents will be less likely to happen in the future.

This relationship between proactive and reactive aspects of the Information Security process is visualized in the following figure.

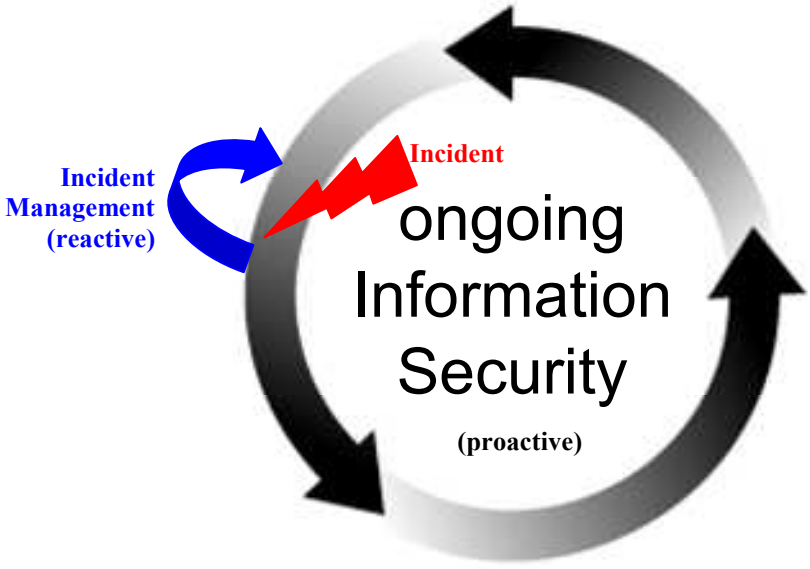

Fig 5: Proactive and reactive parts in an ongoing Information Security process

While most components of Information Security that have been discussed so far are easily classified as either proactive or reactive, some examples of the former in Information Security are training, audit, and any kind of classification. An example for the latter category is incident management. There are also mixed components, e.g. penetration tests, whose goal is to test the current level of Information Security in a company in order to avoid the damage of a real incident (which makes them partly proactive); they do so by identifying faults in the current state of Information Security while also providing feedback that leads to updates of the current state of Information Security when any faults are identified (which makes them partly reactive).

4.7.2 Regular reviews

The only part of an Information Security policy that can be viewed as carved in stone is the policy statement, as it presents the top-level expectations of a company's management regarding Information Security. Since it is the nature of an Information Security policy statement to be easily approvable by anyone who reads it, while at the same time purposely neglecting details, it is highly unlikely for a policy statement to be changed very often.

Procedures and guidelines, however, need to be reviewed more often and on a regular basis. This is an important pre-condition for keeping the quality and efficiency of an Information Security policy implementation on a continuously high level. The materials in question should be approached in the same manner as any pre-existing material on Information Security (details on this approach can be found in chapter 5.2.1). Material in need of updating (e.g. because it does not address the current level of technology in a given area or field) should be

brought up to date immediately. Moreover, all materials should be critically reviewed for their practical use in the current state of Information Security and, if none can be found or the creation of an entirely new version of that material makes more sense, should be discarded. A pre-condition for being able to do so, i.e. to judge whether material is outdated or useless, is continually keeping up-to-date on Information Security topics and issues (as described in chapter 3.2.8).

If sufficient man-power and budget is available, establishing a policy review committee is advisable in order to make the process of reviewing more efficient. Members of this committee should be employees from all allied departments listed in chapter 4.1, most importantly of the help desk department. It is, after all, the people from this department who hear about people's complaints regarding Information Security first-hand, which makes them very valuable in the process of regularly reviewing and evaluating Information Security policies.

In case of updating or discarding Information Security policies' content, one should keep in mind that this content was probably part of already well-established policies which were implemented successfully. What this means is that the content that one is trying to change has likely, if implemented successfully, become conventional wisdom and is remembered by all employees as part of their awareness for Information Security (which is, after all, what the former responsible for these Information Security policies, probably oneself, was aiming for). Changing it is therefore something that must not be taken lightly and entails the danger of employees losing respect for the Information Security department. This danger is especially pressing in case of changes that are drastic insofar as they contradict what was previously an integral part of the Information Security policies.

5. Recommended approach for the implementation of Information Security policies

Up to this point, this thesis has covered the theory of information handling as well as issues and challenges that present themselves during the implementation of Information Security policies. This chapter builds on the previous discussion and presents an approach to overcoming these challenges, providing practical advice and specific solutions to issues one might encounter in the process of implementing Information Security policies. This approach is visualized by the following process model:

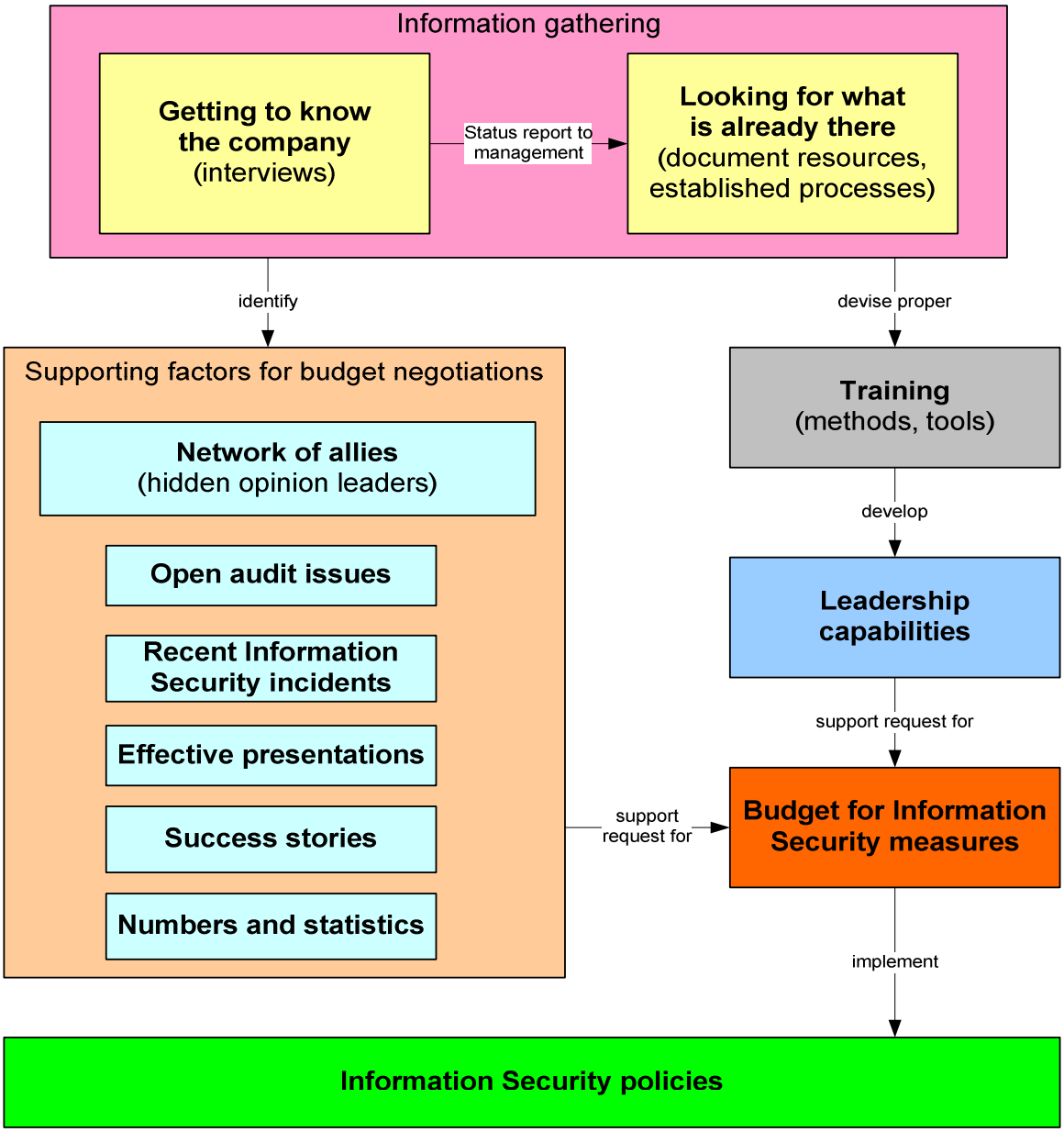

Fig 6: Process model for implementing Information Security policies

The process begins with the gathering of information. This leads to the identification of factors which will later support one's negotiations over budget for the implementation of Information Security measures. The most important factor in this part of the process is the identification of allies. In addition, proper training measures have to be devised, leading to the development and demonstration of leadership capabilities regarding the implementation process. These capabilities, along with the identified supporting factors, help in acquiring the budget for the implementation of the necessary measures that are part of Information Security policies.

Each of the above-mentioned steps within this process will be explained in detail in the following sections.

5.1 Getting to know one's company

In terms of its procedures and sequence, the process of implementing Information Security policies is comparable to any other project. The first step is to understand one's surroundings so as to devise a strategy to implement the project in question (i.e. the implementation of Information Security policies). While obviously an understanding of management's view on Information Security is of importance for having an Information Security policy in the first place, one must look both deeper and closer. That involves checking the surroundings not only for ways that can help with the task at hand, but also to gain a better understanding of how Information Security is being perceived at different levels of a company's hierarchy.

5.1.1 Interviews with management

It may be hard to grasp for many professionals not only in Information Security, but security in general, that the factual necessity for the implementation of security measures and what management deems to be necessary may be two different things entirely. Therefore, the most important aspect during this phase of interviewing is not so much trying to convince management of anything that may be necessary in one's expert opinion, but solely to gather information about the views and expectations of management as to Information Security, identifying any of the company's 'sacred cows' that are a high priority (irrespective of whether they may or may not deserve that status) etc.

The result of these interviews, after being put into realistic terms (that is what the second meeting with management is about) and proper wording, will later constitute the content of the Information Security policy statement. At this early stage, however, the focus is not on putting this into such terms, but, as has been indicated, solely on gathering expectations and identifying what is important to management. The results present one with a clear picture about what, in management's point of view, would be seen as a success in the context of Information Security (e.g. the fulfillment of management's expectations). While an Information Security professional may or may not agree with this view (not only depending on the level of realism in management's expectations), producing a 'success', if taken care of soon, may give him or her an opportunity to establish a good relationship with management.

Such a relationship will serve as a foundation for further Information Security measures that are, in his or her expert opinion, more vital to protecting the company's information assets.

5.1.2 Interviews with other departments

Given the company-wide impact of an Information Security policy, there are a number of departments that can influence its implementation. After obtaining a picture of management's views on Information Security, it is time to conduct interviews with these departments in order to see how they can help and support this process. The goal is to find common points of interest that can motivate people to support each other in resolving issues that affect all participants. From the perspective of an Information Security professional, this means listening for the concerns of other departments and colleagues while trying to find a common ground to form an alliance based on the resolution of these concerns. Such an alliance should address these concerns in such a way as to provide motivation for colleagues to help, while it should also enlist them as allies in one's own agenda regarding Information Security – or at least not make them an obstacle. One important thing to remember when talking to others, in the rather colorful wording of Desman (2002 [2001]: 38), is this:

> "Toes not stepped on are toes that need not be kissed at some later date."

If such an alliance is not possible, e.g. because of too differing fields of work, one should at least leave a good impression with the colleagues as well as having presented oneself as 'the face of Information Security' in the company. This is important because it saves Information Security from being something anonymous and associates it with real people, colleagues whose job it is to protect a company's, i.e. everybody's information assets. Ideally, this will make it less easy to be ignored while also presenting a go-to point in case of questions on the subject of Information Security. For that reasons it is important to communicate in all such meetings how one can get in contact with the Information Security department, who the people are that work there, and that they are always available to answer any questions or listen to concerns regarding Information Security.

Besides making valuable allies, talking to colleagues in other departments in an informal fashion (e.g. during coffee breaks) is a good way to get input about how to best proceed with a project such as the implementation of Information Security policies. Chances are good that some colleagues in other departments have worked in similar projects and are willing to share their experience regarding the existence of experts and hidden opinion leaders (within their own department or somewhere else within the company), the company's management style, aspects that are particularly important to management but that they would not mention in direct conversation, challenges in budget acquisition, etc. In addition, such meetings can give one an impression of the way Information Security has been communicated to employees so far. This is particularly important because it identifies potential shortcomings regarding the seriousness and importance in people's perception of Information Security that may have been made until now. Due to the informal nature of this, it is important not to give these meetings the appearance of an official interview, but rather of a networking activity with the

aim to learn more about a company's employees, its culture and the ways projects are usually handled in this company.

Every company has its own culture which determines how things are run within its boundaries. It is important to know about this, keep it in mind and go *with* that culture, not *against* it, as that would not only increase the resistance of one's colleagues who may have long learned to accept and even be a part of that culture, as well as the resistance of management that surely contributed to forming that company culture and may not be pleased to see any disruptive factor in it. It may prove difficult not to be seen as such, considering the downside of Information Security, i.e. making work processes more complicated than they already are. Yet with the right support on one's side, it is possible to implement Information Security effectively without disrupting the company culture.

5.1.3 Informing management about the current status and planned course of action

After having talked with colleagues from different departments about the company culture, how projects are being conducted and (hopefully) making some allies, one should have a clearer picture of the challenges that may present themselves during the course of implementing Information Security policies as well as management's initial expectations and how they can be met.

The next step is primarily about three things:

- Forming management's expectations into what can later be put into the company's Information Security policy statement;
- Informing management about the status of the undertaking, including results and conclusions based on the interviews with other departments;
- Presenting concrete, planned steps to meet management's expectations.

Since the Information Security policy statement is the foundation for all further documents of an Information Security policy, once one has a clearer picture of the surroundings that will be affected by it, it is best to formulate it so as to create that basis and proceed from there with all further Information Security efforts. Knowing management's expectations and view on Information Security after the first interviews and being able to anticipate the impact it will have on the company by having talked directly to colleagues from different departments, one should make a draft of the Information Security policy statement and present it to management for approval. This may require some revising and updating until management is completely satisfied with the resulting policy statement. This is not only understandable, but also serves one's purpose: By writing the policy statement up in a clear, understandable and specific terms, management will more likely remember its content at a later date, after having approved it, as well as continuously and openly be supporting it once it is released to the company.

As for concrete upcoming steps, it is equally crucial to understand that some of the points addressed during this process may or may not be of vital importance for Information Security.

However, the fact alone that they have been labeled by management as ‘important’ is reason enough to give them, at this early stage, a high priority, especially if these are points that can be addressed with relatively small effort or if they address open audit issues. By doing so, one can quickly achieve a few ‘easy successes’ which, regardless of their actual importance for a higher level of Information Security, will document the importance of Information Security in the eyes of management. This may likely benefit any further Information Security efforts dealing with subjects of higher actual importance, because once management acknowledges Information Security in general as something of importance, it is more likely to also grant the necessary budget for maintaining it. Addressing these points first and then moving to the more important ones is therefore a good foundation to begin the overall process of implementing an Information Security policy.

This is equally true for points that have been identified while networking with colleagues in other departments. If they get addressed as soon as possible, this will gain a lot of favors in the corresponding departments, especially if they address an open audit issue, enhancing the good relationship these departments have with the Information Security department.

Obviously, one has to create a list of priorities here. Contrary to what one might expect, this list should not be primarily prioritized with regard to the highest Information Security importance, but should list those tasks that will contribute most favorably to the perception of the Information Security department, especially by management responsible for budget allocation. This stage is therefore something of an advertising effort. In the long term, getting these tasks handled first will make others that would otherwise be much more difficult to implement considerably easier, because one can thus draw on the support of all the other departments whose problems one has helped to solve. An obvious exception to this rule are clearly critical Information Security issues that have been identified during the interview phase which should be addressed as soon as possible because they pose an immediate threat to the company’s information assets. These should be communicated to management with all the urgency they deserve and also be addressed as soon as possible, before all others. If that requires the cooperation of other departments, this cooperation must be obtained, even if by management’s orders. Moreover, an aggressive timeframe should be set up to solve these issues.

5.2 Looking for what is already there

As has become apparent by now, implementing an Information Security policy is a task that is met by a number of challenges. A vital part of this implementation process is – out of a sheer sense of efficiency – to look out for any resources that are already available within a company that may provide some insight or advantage as to overcoming these challenges. In some cases others may already have invested their time and effort into Information Security or probably document materials related to it. It therefore makes sense to look for such materials, i.e. documentation, but also for procedures that have already been established within the company in which one is about to implement Information Security policies.

5.2.1 Looking for document resources

There lies no sense in reinventing the wheel. Based on that principle, it also makes sense to determine if there already exist document resources at a company that can be used to support the process of implementing Information Security policies. Such resources may be:

- Old policies (policy statements, standards, procedures, guidelines)
- Documentation of security tools and procedures that are currently applied at the company
- Documentation about unfinished or abandoned Information Security projects
- Information Security proposals that never made it into a policy document
- Audit reports
- Any other documentation related to Information Security

Old policies (policy statements, standards, procedures, guidelines): Old policies (more precisely policy statements, standards and procedures) are extremely valuable in that they offer insights into what seems to be dysfunctional in a company's current state of Information Security (else there would be no need for the implementation of new Information Security policies). They therefore serve as a negative example that can be studied for the identification of factors that may be responsible for its ineffectiveness and the need for new policies.

Guidelines are different from policy statements, standards and procedures in that they focus on very specific topics and need to be analyzed accordingly. Their usefulness is decided therefore not so much by seeing them as part of the overall Information Security policies, but by judging them in isolation from the other policies' documents. For example, a guideline explaining secure data handling in Windows 98 nowadays has no relevance whatsoever, no matter what Information Security policies it is a part of (although the existence of such a guideline might suggest that the policies themselves could use some updating). On the other hand, a guideline explaining in general terms the creation of secure passwords has its relevance even though the Information Security policies it is a part of may lack efficiency for reasons that have not been identified yet (the guideline in question likely not being one of those reasons).

The directive concerning document resources that have been found is simple:

"Use what you can, discard the rest."

When doing so, however, one has to keep in mind that discarding document resources in particular is a highly sensitive matter if the original authors of these documents are still part of the company. It is highly advisable to look up the original authors of a document that is being reviewed for its reusability and consult them on the content of that document in terms of the new Information Security policies. This is not only a matter of diplomacy, as in many cases these documents have also a sentimental value to their authors who might be offended if their work was simply discarded without their acknowledgement, but also a chance of making these people valuable allies in updating 'their' documents or presenting an entirely new

version. Again, one should follow the principle as quoted before: “Toes not stepped on are toes that need not be kissed at some later date” (Desman, 2002 [2001]: 38). However, if updating an old version of a document requires more effort than writing a new version from scratch, the old version should be discarded for obvious reasons.

Generally, if looking through materials and deciding whether to keep, update or discard them, one should ask the following questions (based on Desman 2002 [2001]: 45) before reaching a final decision:

- Does the material reflect the environment as it exists today?
- Is the material located so as to be readily available to the people who need to access it?
- Does the material refer to systems or processes currently in place?
- Is the material presented in a form approved for a company policy and company procedures?
- Is the original author still around?
- Will the old documentation fit into the new standard?

Documentation of currently applied security tools and software: If any security tools or software are currently being used within the company that have to do with Information Security, their application and documentation needs to be verified to see if it is compatible with the Information Security policies about to be implemented. The choice for a particular security tool or software in question was likely taken for a number of reasons. Therefore, as before, in case that the tool/software is to be discarded or its current application drastically changed to fit new Information Security policies, advance consultation with the person that was originally responsible for the decision to implement it is not only a matter of diplomacy, but can provide valuable information regarding that choice.

Documentation about unfinished or abandoned Information Security projects: Some Information Security projects are never completed or even reach the final implementation phase. That can happen for a number of reasons, yet sometimes the initial idea that started the project was generally valid. Information of such nature is to be found in the project’s documentation. After studying this documentation and talking to the people who were responsible for the project, it may be re-evaluated and even revived because of its worth in supporting a company’s Information Security program.

Even if it does not come to such a revival, the people responsible for the original project may make valuable allies in any case, as they likely know some details that led to the project’s termination and that could be worth knowing for pursuing similar projects in the future (e.g. unforeseen budgetary complications, opposing opinion leaders etc.).

Information Security proposals that never made it into a policy document: In some ways similar to the case described above, proposals for Information Security are efforts that were suggested, yet never made it into an official Information Security policies document. Taking

the time to talk to the people who were involved in such proposals and looking up any documentation about them could, for the same reasons as above, reveal that the initial idea was one that would be worth pursuing in the present.

Audit reports: Information Security audit reports are immensely valuable for two reasons. First, they contain a history of some of the company's flaws regarding Information Security, meaning that flaws that have been identified already some time ago are traceable in detail through their corresponding audit reports. Second, audit reports normally go directly to management and receive a high priority on a manager's schedule. That is because audits frequently check on a company's fulfillment of legal or certificate requirements, i.e. the pressure on management to fulfill these requirements is high. Open audit issues are therefore treated with high priority by management which makes management cooperation along with the necessary funds very likely if one was to present a solution to such an issue in the course of implementing Information Security policies.

While reading such reports, one needs to be aware that, besides the flaws that have been identified by the auditor while checking the fulfillment of requirements to reach a certain legal or certificate requirement, an audit report may also contain other flaws that the auditor found in the process of auditing, along with further recommendations as how to deal with them.

Any other documentation related to Information Security: Any other Information Security-related material that can be found throughout the company needs to be identified. Knowledge about this material is of great importance, because it may not only reveal the current state of a company regarding Information Security, but allows one to decide on updating or removing this material, if necessary. At the same time, one needs to keep in mind the above-mentioned checklist of questions for such a case and the rules of diplomacy with colleagues in the process of discarding any material.

The distribution of such material happens through a company's internal media and communication channels. Knowing about these channels, i.e. where and if such information was released, whether it was published, how often and by whom, is of vital importance for a later use of these very channels to distribute one's own Information Security content. Especially the responsible people need to be consulted because they likely not only control these channels, but also have knowledge about the content that has been published using them so far. These people make some of the most valuable allies in the process of implementing Information Security policies.

5.2.2 Looking for established processes

Besides documentation materials, another thing to look out for while identifying potentially useful assets that are already in place within a company are processes that have been established for some time. These processes often become part of a company's culture over time. As they have become an accepted (although probably not acceptable, at least in terms of Information Security) way to do things, changing these processes is one of the most

challenging issues that has to be dealt with during the process of implementing Information Security. While interviewing management and networking with colleagues from other departments, one should identify the processes that are most critical in the eyes of management. These generally fall into two categories, official and unofficial.

Official, established processes: Official processes are processes that are the result of process-building and/or process-optimizing efforts previously conducted in the company. While the core idea of these processes, i.e. the reason for the process to exist, may work within a desired range of efficiency, this does not necessarily mean that the level of Information Security in this process is equally satisfactory. In a worst case scenario, Information Security may have even been left out entirely of a process in order to make it more efficient in its core functionality.

Presenting Information Security as a necessary addition to these processes often results in a reduction of its core efficiency. As a result, the tendency to resist any change in these processes that might endanger this core efficiency may be strong, depending on the importance that this process is given by a) management and b) the people directly involved in it.

Unofficial, established processes: Not everything that is regularly handled in a specific way within a company constitutes an official process that was deliberately built at one time and updated at another. Many processes exist besides official ones, connecting them to make the whole of a company and its efficiency what they are. Unfortunately, what goes for official processes in terms of Information Security goes also for unofficial ones.

Identifying unofficial processes is a lot harder than official ones in that no documentation on them exists and in that they change constantly as the circumstances around them evolve. A good example for such a process is the consulting of a hidden opinion leader. No document contains any rules or regulations that state that this particular person has any real decisive power, yet in the real world everyone at the company knows that he or she does, simply because of his or her expertise in a specific field in question.

Generally, the only people that know about these processes are the people involved in them. While talking to colleagues from other departments and networking with them, it is important to keep an ear out for hints about such processes and delicately investigate them in order to verify whether they do or do not violate the Information Security policy.

The implementation of Information Security policies in regard to both types of processes, official or unofficial, may be – for the most part, as has already been indicated – seen as a sales matter. In this, Information Security is the object of bargain (i.e. a necessary addition to an already existent product, the process in question), the responsible Information Security professional acts as a ‘salesman’ (or ‘saleswoman’) and the company’s employees, respectively their managers, assume the role of prospective ‘buyers’.

5.3 Finding allies and gaining their support

The importance of finding allies and gaining support has been pointed out throughout this thesis on numerous occasions. Indeed, this can hardly be over-stated, as this is probably *the* most important thing to be done if the implementation of Information Security policies is to have a reasonable chance of success. Without it, failure of this process is virtually unavoidable, as Information Security becomes an isolated struggle against an overwhelming mass of potential adversaries – for that is what other employees will mostly become if not convinced of the need for Information Security. This can only be achieved with the help and the support of allies throughout the company.

Chapter 4.1 of this thesis focused on the principles and the importance of company allies within the following departments:

- Human resources (HR)
- Information Systems
- Public Relations (PR)
- Documentation department
- Internal Audit
- Legal and Compliance department
- Application Development
- User Management and User Support
- Operations
- Corporate Security
- Facilities
- Graphic Art department
- Finance, Controlling

What follows is a detailed discussion of each of these departments and the ways each can support the implementation of Information Security policies. The basic principles that apply here are are:

‘Let others do what they do best.’

‘Let others be the eyes and ears of Information Security everywhere.’

5.3.1 Human resources (HR)

The department of human resources (HR) has responsibilities that share a deep involvement with Information Security. These responsibilities (the most important of which, in terms of Information Security support, are listed below) reach out to the farthest corners of a company, making this department one of the most powerful allies one can have within a company. Here are some of the ways in which HR can support the process of implementing Information Security policies:

Information distribution channels: HR is the perfect ally for the distribution of Information Security content which can be published through various channels that are usually controlled by HR. These channels are often used to distribute the same information redundantly (sometimes varying in length and detail of a message), so as to have a greater chance of actually reaching their targeted audience. They are defined and differentiated from each other by the following aspects:

- By the media that serves as a carrier for that information (e.g. E-mail, printed hand-outs)
- By the content carried through that media
- By the frequency of use of the carried information
- By being event- or incident-based or regular

Generally, one should monitor all channels of information content distribution controlled by HR and look for opportunities to place Information Security content there. In such cases, any kind of information that goes through these channels should contain a purpose-designed Information Security logo to make it immediately recognizable for recipients as containing Information Security content.

Some information distribution channels usually controlled by HR are:

- Company newsletters: These can be either in E-mail form, which is more common these days, and/or a printed version. The advantage of E-mail newsletters is obviously the speed at which Information Security content can be distributed among an almost infinite number of people. Printed company newsletters are still being used, but not as frequent as E-mail, because printing takes longer and costs more than simply sending an E-mail to a distribution list of recipients.

  As Information Security responsible, one should see to getting a fixed spot in the company newsletter which can be filled regularly with Information Security content (with help of the Documentation department). This content should not, especially in case of a printed company newsletter, be something of immediate importance (e.g. a warning message about a recent Virus outbreak) or something that becomes outdated quickly, but rather something that has a general, enduring meaning (e.g. “10 hints on how to create a secure password”). Also, written articles should always be sent to HR with a sufficient amount of time in advance, so as to build up a reputation with HR as someone who can fill a certain area of their newsletter with high-quality (thanks to the Documentation department) articles about interesting topics delivered on time.

- Bulletin boards: Printed messages posted on bulletin boards are useful in that they can present content in areas of a company where they are clearly visible to groups of employees, also in a non-working context such as in a kitchenette. Such messages are not restricted to bulletin boards, but can also be posted on elevator walls, entrance doors etc.

Advantages of bulletin boards lie in their access to groups of people which can lead to stimulated discussions among these people about the content that is published, i.e. making it a topic of notice that will be remembered more readily.

A disadvantage of bulletin boards is the fact that keeping them up-to-date, especially in a large company, is a considerable effort due to the sheer number of boards, yet it is a necessary effort if bulletin boards are already being used to spread information. A bulletin board that is not updated regularly condemns its content to the fate of being perceived as nothing more than wallpaper that has been hanging there for a long time. Employees simply become used to it hanging there so that after some time they hardly notice it any more. This is something that needs to be considered before thinking about using bulletin boards. If the effort of keeping them up-to-date is too much for a company to handle, it is better to abandon them altogether and switch to other information distribution channels instead.

- E-mail distribution lists: A company's E-mail newsletter is usually directed to all employees of a company. However, some information content may be directed to specific groups only. In such a case, E-mail distribution lists make more specific information channels for different employee groups or about specific topics.

  In case of Information Security, it is important that any E-mail containing Information Security content should be made clearly recognizable as such by using a specific E-mail subject prefix, e.g. using square brackets:

  To: allemployees@company.com
  Subject: **[InfoSec]** Virus alert concerning Virus XYZ

- Intranet web page: The intranet web page is a place for HR to place any company-relevant information, be it of immediate concern to employees or not. It normally contains all recently published information categorized into different sections of topics and concerns.

  One of these sections should be Information Security. By using an Information Security logo and flashing headlines for recent Information Security issues of interest (not forgetting, of course, the rules of good web page design!), immediate attention to this section should be assured, sparking the reader's interest and granting easy access to a company's very own Information Security web page. This web page should be maintained by the Information Security department itself and contains useful information, guidelines etc. designed to capture the reader's personal interest for the topic of Information Security. It should be available in different languages, if necessary, using predefined language templates.

- Intranet user forums: As part of an Intranet web page, user forums can function as a place where employees can post messages to each other about all kinds of topics. The fact that these forums may be visited frequently by employees makes them a useful

channel for information distribution as well as information collection. By generating topics, e.g. about Information Security, HR or other departments are able to publish their content while also follow the reactions of employees. This gives valuable feedback, especially if the topic is security-related, as to employees' level of knowledge of a specific topic as well as their views and attitudes towards it.

Having discussed the advantages of Intranet user forums, their disadvantages should also be mentioned. First, some users in Internet forums have a tendency to improper behavior that might lead to unpleasantries such as personal insults or so-called 'flame wars'. This term refers to heated discussions including insults among users that may have started about an original, specific topic, but have left that topic far behind and now focus mainly on personal issues among users. In order to keep that from happening, a so-called 'netiquette' – a code of conduct – and moderation of user forums is required. This is a task that requires additional effort and resources by HR which makes the decision to establish a user forum a matter of some discussion.

Another common tendency of users in user forums is to talk among each other about non work-related topics. While that may be acceptable up to a certain level, controlling that level also means additional moderation effort for HR. If the number of non-work related topics is much higher than that of work-related topics, any effort by a HR forum moderator to remind users of the original intent of the user forum will most likely be met with some reluctance by the forum's users. What is more, some users tend to spend a lot of time in such forums, thereby deflecting them from their actual duties.

While a user forum integrated into a company's Intranet web page has its benefits in presenting relevant topics and following the reactions of users to these topics, the above factors (moderation effort, employees' deflection from duties) might very well lead to the decision not to establish a user forum.

- Computer message pop-up windows: In some cases it may be necessary to immediately inform employees of something as soon as they access their computer by logging into the operating system. If they do, a message window pops up, e.g. informing them of an upcoming software update, a recent computer virus outbreak etc.

  This kind of information distribution should be used mostly for computer-related issues and only if a certain level of urgency is present. One advantage of this method is that it presents HR with the possibility of obtaining a user's acknowledgement of the message that has been sent by attaching a button saying 'I have read and understood this message' that appears and prompts the user to check it in order to make the pop up window disappear. This possibility, however, also holds a disadvantage, since many people react negatively to pop up windows as a result of the many advertisement pop up windows they encounter while surfing the Internet. These are usually seen as an annoyance and 'clicked away' as fast as possible (if not blocked entirely by pop up blocker programs), mostly without reading the message at all. Such

a reaction or even the corresponding attitude is, of course, not desirable for a company-related message transmitted over a pop up window, yet the relation between both kinds of pop up windows is undeniable, making the use of this kind of information carrier a subject for discussion.

- Seminars, talks, Webinars: HR is responsible for the organization of seminars, informative talks and Webinars through which a certain topic (e.g. Information Security) is presented to employees. These may be stand-alone events, part of a series of events or part of an entire training program. Depending on the topic in question, corresponding departments within a company may be required to participate in its organization. If, for instance, HR organizes a talk given by a renowned Information Security expert, the Information Security department will be involved in preparing this event, documentation materials etc.

Some information may be spread because of a special occasion. Depending on the nature of such an occasion (i.e. event or incident), the urgency of communicating this information calls for the use of proper media for communication. If the message to be distributed calls for great urgency (e.g. an incident warning about a computer virus outbreak), choosing a printed hand-out would obviously be a poor choice for a medium, as such information needs to be communicated as fast as possible. On the other hand, in case of an event such as the appointment of a new CEO or the introduction of a new Information Security policy, a printed hand-out would make a perfect medium for publishing this information.

Another factor in event-based publications is the frequency of use that one specific piece of information content is expected to have. Information material that is being published on employee's Orientation days will be accessed very often and should therefore be communicated through printed hand-outs with the option of downloading a PDF version of the document from the company's Intranet web page.

Employment: HR is directly responsible for almost anything related to employment. This presents one with a set of opportunities to communicate Information Security to employees:

- Recruiting: HR can help in communicating the company's view on Information Security to potential employees even before they actually start working at the company. This can happen by including corresponding messages (e.g. the company's Information Security policy statement or quotes by the company's CEO that illustrate his view on Information Security) into the recruiting materials. These can be accompanied by a statement about the company's recognition for its responsibility regarding Information Security (especially if it is a company that deals with extremely sensitive information such as medical or financial data).

- Orientation days: These events are intended to present relevant information concerning work surroundings and procedures, but also obligations that have to be met (including the signing of a non-disclosure and an Information Security agreement) to new employees. Right at the start of a person's employment is the perfect time and

place to address Information Security as a topic of interest, communicating its importance for the company and the company's expectations to every employee. Chapter 5.5.4 will cover in more detail the inclusion of Information Security messages in Orientation days.

- Training: HR's main responsibility are a company's employees. In many companies, HR is in charge of organizational decisions concerning training for sizable audiences (trainings for individual departments may be organized by the heads of these departments themselves, using the corresponding department's budget). These decisions are, wherever necessary, made in correspondence with relevant departments which provide their professional input on that decision. In case of Information Security, HR would therefore consult first with the company's Information Security department before making choices, e.g. about how to include Information Security in the company's employee handbook that is handed to every new employee during Orientation days. However, since HR has many other responsibilities beyond this, an Information Security responsible should not wait for HR to call regarding such issues, but actively approach HR on the issue of relevant Information Security training and raising employee awareness, as well as actively participate in the arrangement of that training. These arrangements include:

    - Decisions on whether to hire external trainers for employee training (e.g. for Information Security) or give the job to the internal Information Security department
    - Choice of training methods
    - Length and level of detail of training
    - Choice of training materials and documentation

On the other hand, HR might require one's services in the unpleasant event of letting go of an employee if that individual has violated some of the company's policies. Due to one's position in Information Security and connections to other departments, one should be able to assist HR in collecting the necessary evidence for such situations, demonstrating the alliance shared with HR.

Placement of information material: The general nature of the Information Security policy statement makes it *the* document that is most often referred to in questions about Information Security. It lies within HR's responsibilities to place the policy statement as well as any other Information Security relevant information material (folders, posters, printed hand-outs etc.) any place within a company where it is visible and needed. This way the message of Information Security is placed before the target audience (i.e. the company's employees) on a daily basis, raising awareness.

As a final point of interest, the HR department can be of great help during the phase of identifying Information Security-related materials and evaluating them for further use in new Information Security policies, because it knows about most materials that exist and where they can be found.

5.3.2 Information Systems

The Information Systems department's most valuable support for an Information Security policies' implementation lies in running and maintaining technology-based (mostly software) solutions for the protection of information assets. This applies to a variety of measures, from the implementation of a password policy (e.g. requiring the change of a user account's password after two months without using one of the last five passwords that have been chosen) to an extensive authentication system for remote access to an employee's user account and/or information assets.

Some of the ways the Information Systems department can support Information Security are:

- Requirement of new software: In case that the introduction of a new piece of software to protect Information Security is being considered, the Information Systems department should be consulted as its members have the necessary know-how to evaluate the software in question with respect to its suitability to be integrated into the company's information systems.

  Before approaching the Information Systems department with the issue of introducing a new piece of software to the company, the following aspects should be considered:

  - Familiarization: Familiarity is an issue not only with respect to the established systems used within one's company, but also with respect to systems and software that are currently being used throughout the industry for the respective purpose.

  - 'New' does not necessarily mean 'better': Information Systems' responsibility lies in providing stable systems for the company's operations. 'Never touch a running system' may very well be a motto held in high regard by the members of this department. Therefore, one should beware earning a reputation for 'wanting to play with every new toy on the market'.

    New software should be introduced to Information Systems for implementation only after reviewing it in detail and identifying it as a valuable addition in support of Information Security, not just because management requests it. In the latter case, if the software in question would not make a useful addition, one should act as the voice of reason and convince management that an implementation would not be to the long-term benefit of the company.
  - Choosing wisely: If a software implementation would result in a strong, negative impact on the processes involved, it was likely a bad choice in the first place. Alternatives are probably available; they only need to be identified. There are rare cases in which a company has to suffer such a negative impact in order to gain certain software functionality. If the Information Security of a company relies on the implementation of a product that has such a negative

impact on the processes involved, the chosen Information Security approach is likely flawed in its design.

- Advertisement: Depending on the novelty of the software, one should advertise its use throughout the company, creating curiosity as to its functionality and the benefits it will bring to the company, and only at the last moment reveal it to the public.

- Simplicity: The simpler the software is to use, the more it gets used. As a general principal of usability, the more complicated software solutions are, the smaller the chance that they will be used by employees.

- Experience: Anyone with experience in the use and implementation of a specific piece of software as well as training for its use should be consulted. This includes colleagues, other Information Security professionals, vendors, people met at conferences or product presentations etc. Ideally, members of Information Systems should be present during a vendor's presentation of the software to ask questions about its implementation etc.

  Especially vendors should give concrete statements on these topics that one can rely on after obtaining the software. They can also help out with presentation and training materials that will be needed after the implementation of the software.

- Data provision: Another important responsibility of Information Systems is providing automatically generated, Information Security-relevant data, e.g. the number of times a company's Information Security web page has been accessed by employees per month. This kind of data is relevant as it expresses the efficiency of a company's Information Security in numerical values. This is especially important during budget meetings in order to present the current status of Information Security to management. Chapter 5.6.6 elaborates on this as well as other statistical and numerical values that can support one's position in such situations.

- Information Security web page setup: Setting up an Information Security web page will most likely be done at Information Systems as that department will provide the necessary resources (web server, web space etc.). This should be done in accordance with the Graphic Arts department in case the design of that web page is done by that department, as well as HR to secure a place for a link to this web page on the company's Intranet web page.

5.3.3 Records Retention

Backups and archiving are two of the most neglected areas when it comes to Information Security. While information handled within current operations may be dealt with on an adequate level of Information Security, as soon as the same information is no longer involved

in these current operations, but is being backed up or archived, i.e. put into the background of current operations, this level of Information Security is often drastically dropped for no particular reason. The error committed here is based on the false assumption that just because information is no longer ‘in the spotlight’ (i.e. involved in current operations), where it receives an adequate level of Information Security, its value is less than it was before. This is incorrect insofar as the data contained in a backup or archive was, not so long before, part of current operations and therefore highly protected by Information Security. This makes backups in particular a very attractive target for Social Engineering attacks, because the level of protection for backup systems is often neglected not only in terms of Information Security, but also of physical security (i.e. backup systems are stored in an area that is physically less secure than the location of productive information systems).

The Information Systems department, together with Records Retention and Information Security, can join efforts to make *all* of their systems and data processing operations (e.g. backup operations) sufficiently secure in terms of Information Security (e.g. by using cryptography). Such an effort involves not only productive information systems, but also backup and archive systems.

Moreover, with help from the Legal and Compliance department, one should make sure that the Records Retention department knows about and adheres to the current legal regulations about archiving sensitive information data (e.g. customer information) and handles the destruction of information carrying media properly.

5.3.4 Public relations (PR)

Regarding Information Security, it is PR’s responsibility to present a company to the public as handling sensitive information data (e.g. customer or research data) responsibly. This serves two purposes:

- To attract new costumers and ensure established customers by giving them a sense of security when it comes to data they entrust to the company.
- To ensure shareholders that with the level of Information Security currently present within the company, the chance of an incident based on a failure of that security, which might lead to a potential drop in the company’s share value, is kept to a minimum.

5.3.5 Documentation department

The Documentation department is usually one that the Information Security department should constantly be in very close contact with. The reason for this is that all publications regarding Information Security should first be reviewed by that department, its job being to optimize the content before it goes public in terms of readability, proper wording and the company’s overall style for such documents. While this service is undeniably vital to reaching a target audience, one should always double-check a document version that has been corrected by the Documentation department and assure oneself that, besides the corrections

that were made to the wording, the original message to be communicated is still intact. If that is not the case, the document needs to be updated accordingly and sent back to Documentations with an explanation of the facts that were lost during the last correction. This may go back and forth for some time, yet in the end will result in a document that both contains valuable information and is easily readable for anyone it is presented to.

In order to make this process more efficient, one can draft Information Security documents in a way that minimizes the corrective effort for the Documentation department, i.e. saves time in finishing the final version of these documents. This can be done by following these hints:

- Taking writing classes: This is generally a good idea, since the better the draft of a document, the less time and effort is needed in correcting it by the Documentation department. The fact that a great number of people are going to read one's writing makes this a worthwhile investment of effort and should serve to highlight the general idea that – even in the first version – each sentence, each word should not be chosen carelessly, but purposefully.

- Writing simple: Information Security documents should be written as simple as possible. No complex vocabulary shall be used. As a point of reference, one should write for 14-year-olds, using simple and understandable sentences so that only basic prior understanding of the subject is required to follow the document. The aim should be to deliver a message, not write a novel or a PhD thesis. The reader's effort to understand the text should only be about content, not about the language or style of the text.

- Exemplary situations: In order to maximize acceptance by readers, the content should include the description of situations in which a reader may find him or herself, so that identification with that situations is facilitated.

- Humor: Adding humor and entertainment (e.g. comic strips) to an article may give the message to be delivered a better chance of being remembered by the readers.

- Spelling and grammar checks: Since they are offered by any office suite software currently on the market, one should definitely use both spelling and grammar checks before forwarding a text to the Documentation department. Its employees can then focus on correcting errors in style or wording (which is their area of expertise), instead of errors that could easily have been taken care of by running a spelling and/or grammar check. This avoids placing additional work on the Documentation department, which they shouldn't have to do anyway. To neglect the use of spelling and grammar checks can moreover hurt the alliance with this department, because it gives the impression that one does not care enough about what to deliver, knowing that it is going to be corrected by the Documentation department anyway.

- Audience's cultural environment: Awareness of the readers' cultural environment is important in the choice and presentation of the content put in front of them. Not all

content is equally relevant to readers coming from different cultural backgrounds (e.g. a comic strip intended to amuse the audience of one country, but emphasize a certain subject in Information Security, might offend the audience of another country because of cultural differences). Yet, since it has its relevancy for the company, if and when dealing with readers from different cultures, one has to take this fact into account while thinking of the best ways to communicate the message to all of them.

- Logo, contact information: Each article that is being published should contain a clearly visible logo of the Information Security department that makes this article immediately recognizable as containing Information Security content by anyone who so much as glances at it. Additionally, all materials should offer ways of contacting the Information Security department (name of the author, E-mail address and telephone number).

Besides that, the Documentation department's support of Information Security can consist of:

- Identification of old documentation materials: Since all materials that have been published in the past have (or should have) passed through the Documentation department, looking there for clues about the whereabouts of any existing Information Security-related documentation material can be of great help in identifying old materials that might still be of use for new Information Security policies.

- Identification of Documentation employees specialized in Information Security: Since Information Security is all about publishing materials, especially in bigger companies the Documentation department will allocate one or two members to dealing with enquiries from the Information Security department (among other topics). Over time or maybe even through proper training, these individuals will obtain a deeper understanding of Information Security matters than the average employee and will therefore be able to put this knowledge to use during their editing and corrective work. Needless to say, having such colleagues as allies in the Documentation department significantly reduces the effort of sending back and forth Information Security documentation drafts.

- Translations: In some cases, where employees of different countries need to be addressed, translations of one's written material may be required. The Documentation department usually knows how to best accomplish this or who should be assigned to this task. In case of translations for online materials on the Intranet or Information Security web pages, this is best done by using language templates. To use such templates, it is necessary to consult with Application development or Information Systems, depending on who is responsible for the technical development and maintenance of the Intranet web page.

- Printer-friendly version of online documents: In case that employees want to print out content that has been published on the Intranet or Information Security web page, printer-friendly versions of all materials should be made available for download, and a

corresponding link be placed that is clearly visible next to the article published online. These printer-friendly versions should be edited separately by the Information Security department in terms of style and appearance.

5.3.6 Internal Audit

The role auditors may play in one's effort to successfully implement Information Security policies has partly been discussed in chapter 4.4.1. While the present section focuses on the Internal Audit department's role as a necessary ally for the Information Security department, many ideas about the relationship between auditors and the Information Security department apply equally to both internal and external auditors.

When the Internal Audit department does an audit, it faces a problem that external auditors are probably glad they do not have to share. When external auditors leave the company building after their final presentation to management, they know that their work is done and that whatever consequences will result, this does not concern them. Internal auditors, on the other hand, are part of the same company as the departments they audit. This means that not only are they expected to have a much better understanding of the company in the field covered by the audit, they also have to live with the consequences of their findings after they present them to management. This can lead to a very hostile atmosphere between the Internal Audit department and the rest of the company.

Mark B. Desman describes two types of internal audit scenarios (Desman, 2002 [2001]: 206):

- The 'feel good' audit: In this scenario, realizing the above-mentioned problem, the Internal Audit department deliberately avoids going beyond the surface of the problems it encounters during the audit in order not to expose or offend the other departments before management. In order to maintain a good working relationship, the so-called audit becomes something of a fraud, because real issues that threaten a company's assets are not properly dealt with, maybe not even identified, only to 'keep the peace'. Naturally, this approach to an audit is not very efficient as its results only present a fraction of the real issues present at a company and likely also lack the details on the true damage potential of these issues. Also, the issues that are reported are most likely not the most critical ones, as exposing these would probably disturb the relationship between Internal Audit and the department where the issues were uncovered.

  In a 'feel good' audit, everybody involved stays more or less happy (i.e. feeling good):
  - The auditors can pretend they are doing their jobs and present results that seem reasonably enough to make management think that these are the only issues uncovered during the audit.
  - The departments that have been audited are satisfied as either no issues have been found by the auditors, or those that have been found are not critical enough to be seriously uncomfortable.

    - Management rests in a false sense of security, knowing that an audit has been performed, some issues have been found and will be dealt with.

  The only victim of such a 'feel good' audit is obviously Information Security.

- The 'avenging angel' audit: In this kind of audit, an internal auditor feels the urge to uncover everything there is to uncover at a company within the scope of an audit. While such an eager attitude is not a problem of itself, it can become one if the general attitude of the auditor is such that he or she thinks him or herself as an 'uncoverer of issues that auditees are trying to hide'. Such an attitude communicates clearly hostile intentions towards the audited departments, because the primary goal of the audit is no longer to benefit the company by uncovering potential threats to company assets. Instead, as a reaction to this attitude, auditees tend to do only what they are expected to by the auditor – which is hiding issues that, if they were exposed, would make the responsible department look bad in the eyes of management. The audit therefore becomes something of a 'private war' between auditor and auditees over the exposure of these issues that are assumed to have been hidden on purpose by these departments (which may even be true). While, on one side, the departments that are being audited take satisfaction in the auditor not uncovering these issues, on the other side, the auditor takes satisfaction in trying to do just that and proving these intentions futile.

  Due to the lack of cooperation between auditor and auditee (which in such a scenario is practically non-existent), this kind of ego-driven competition has one clear victim: Information Security.

Since both these scenarios are inadequate with respect to both producing reliable audit results and doing so in an efficient manner, the roles of internal auditor and auditee within a company need to be redefined.

The solution to this necessity comes with the realization that the auditors' and the Information Security department's goals are very much alike. Essentially, the latter tries to fix issues that the first have identified beforehand. Both do so with an interest in achieving a high level of Information Security for the company of which they are both a part. With this realization, it becomes obvious that auditors are in fact simply doing something that would otherwise fall into the domain of the Information Security department itself: In order to address issues, they first have to be uncovered. If auditors can help in this by simply doing their job, such assistance should be more than welcome by the Information Security department and be assisted by all means. While this may not increase their popularity with the departments they need to audit, it gives the Information Security department the opportunity to step into the auditor-auditee relationship as an intermediary between the two parties, acting as what is also called 'audit interface' (Desman, 2002 [2001]: 207).

When it comes to auditing the level of Information Security of a company, what an auditor practically does is to evaluate the work of the Information Security department. It therefore

makes sense that the primary contact for this audit should be someone from this department, serving as ‘audit interface’ between the auditor and other departments that are being audited. The advantages of this approach lie in a reduction of potential tensions between auditors and auditees as well as the provision of first-hand information regarding the current level of Information Security, made directly by the corresponding department.

With this approach to an audit, it becomes imperative not to hold anything back, but to give the auditors everything they need to complete their task, i.e. full cooperation. A problem that auditors frequently face is that they lack sufficient knowledge about the company, its processes and the systems they are supposed to audit. While this applies to external auditors more than to internal ones, the latter also face this problem. This is the case especially in the two scenarios described above, when faced with uncooperative departments which are not only not trying to help, but purposely make the auditor’s task more difficult by holding back information that could reveal an audit issue.

Since an Information Security audit is, in principle, about assessing the work of the Information Security department, any material required for such an audit should be readily available to be handed over to the auditors. In cases where further materials are required, Information Security can obtain these, acting as an interface between the auditors and the departments in question. Thanks to the good relationships the Information Security department has established throughout the company, providing any information requested by auditors should thus be easier, without facing resistance as described in the scenarios above. This cannot happen, however, without first ensuring a general understanding of the auditors’ role in protecting a company’s Information Security. Without such awareness, handing over information about a department can result in the corresponding department feeling ‘betrayed’ by Information Security for ‘siding with the enemy’ (e.g. the auditors). Openly declaring the Internal Audit department as allies and emphasizing their important role in ensuring the safety of a company’s information assets is therefore of immediate importance, even before an audit actually begins.

During an audit, one should regularly check with the auditors to see if they have everything they need and also keep track of their progress of the audit. This way the content of the audit report drafts should come as no surprise. In case that meetings with other departments need to be arranged, one should act as moderator and mediator in case of disagreements. The meeting just before the end of an audit is particularly sensitive. In such a meeting the auditors present their draft of the audit report to all departments involved. Since these reports go directly to management, consensus or at least compromises about their content and wording need to be found so as not to expose or embarrass anyone unnecessarily. Also, knowing the content of the audit report, the departments can already begin to solve the issues that have been found, even before management knows about them. This gives them the opportunity to already have something at hand when management finally approaches them on an issue that has been identified in their department.

The advantages of this approach are not only a higher level of Information Security, resulting from the fact that all efforts in the audit process are being devoted to the discovery and fixing of issues, but also that every party involved in the audit wins:

- The Information Security department gains the assistance of Internal Audit in identifying potential threats against Information Security.
- Internal Audit receives full cooperation and all required materials and is therefore able to perform the audit more accurately.
- The departments where audit issues are discovered have time to prepare for a response before management approaches them.

5.3.7 Legal and Compliance department

The Legal and Compliance department's job is to ensure the compliance of a company's operations with the current state of law. Since these operations are specified by a company's policies, Legal and Compliance needs to make sure that these documents are not in violation of these laws. In the case of Information Security, this means that any document needs to be verified by Legal and Compliance before becoming part of the company's Information Security policies. If changes to these documents are made by Legal and Compliance, it is important to review them with regard to simplicity and the absence of legal jargon. When in doubt, the documents should be sent to the Documentation department for review and then be verified again by Legal and Compliance.
Legal and Compliance is also a valuable respondent when it comes to audits. Knowing that the Legal and Compliance department is there to answer any questions on legal issues is a great benefit not only during internal audits. Especially when expecting external audits, the evaluation of Information Security measures' compliance with the current state of law becomes a necessity.

Other fields of operation for Legal and Compliance are providing information about legally correct retention of costumer data (in cooperation with the corresponding Records Retention department) and communicating with HR about the legal consequences of an Information Security policies violation.

5.3.8 Application Development

Security aspects in the operations of this department fall mainly into the area of Software Security and secure software development. Still, verification of the existence of certain security measures is part of Information Security.

- Verification of COTS software: In most companies, there is a trend to use so-called COTS (commercial off-the-shelf) software, because it is cheaper than developing a customized solution on one's own. This presents various difficulties regarding Security. Having the character of a 'black box' that only needs to be plugged in to be used, one can never be sure how exactly this software has been developed in regard to security. Even if COTS software is used only as part of a bigger software solution, the

applications department needs to verify the security of this software and whether it complies with the security standards used at one's company.

- Recommendations for software solutions or development: If a certain functionality is required to improve Information Security at a company, the Application development department is likely to have advice on plausible solutions that are currently available on the market. If no solution meets the requirements, the software can probably be developed by the Applications Department itself or outsourced to another company.

  In case that the development of secure software by the Application development department becomes necessary, it needs to be informed about the company's legal liabilities in case of loss or misusage of information assets as a result of using software developed by the company. This should happen in cooperation with Legal and Compliance.

Additionally, this department may provide help in setting up an Information Security web page at the web space provided by Information Systems.

5.3.9 User Management and User Support

User Management and User Support are two closely related fields of responsibility and are therefore often located within the same department. While the User Management department's responsibility lies in managing everything related to the employees' user accounts (e.g. creation, deletion, deactivation etc.), responsibility for frontline user support lies with Help Desk. The latter is usually the first point of contact for all employees with any kind of problems they encounter during their company's operations. Thanks to the close contact that Help Desk has to a company's employees, it is in a perfect position to point out the importance of Information Security during its operations.

Since Information Security has the tendency to interfere with the way that many of these operations are conducted, it is likely that some of the problems and complaints that Help Desk encounters during its operations are, to a certain extent, related to Information Security.

The User Management department and especially Help Desk is therefore a good source to obtain information about the following topics:

- The general understanding and attitude of employees concerning Information Security (are they aware of its necessity or do they perceive it as a mere annoyance and. if so, why is that exactly?)
- Operations and applications that repeatedly cause troubles for employees because of Information Security measures

Regular feedback by Help Desk regarding these topics allows one to improve the way employees perceive a company's Information Security program.

5.3.10 Operations

The implementation of Information Security policies at Operations is as relevant as it is elaborate. This stems from the fact that the majority of information that needs to be protected is usually handled through the services provided by the Operations department. This makes Operations one of the departments that are affected the most by Information Security policies. Acceptance of this influence by the Operations department as well as the employees using their services can only be accomplished on the basis of awareness of the need for Information Security measures.
Moreover, in the event that new software supporting Information Security needs to be integrated into existing systems or services, this falls mainly under Operations' responsibility as these systems or services are usually run by this department.

5.3.11 Corporate Security

Corporate Security is responsible for any aspects of physical security inside a company. There are numerous ways in which Corporate Security can assist matters of Information Security:

- Restriction of physical access to sensitive areas: Corporate Security has the means to physically secure access to sensitive areas such as server rooms, backup storage rooms, document archives etc. It is their responsibility to hand out badges to employees, temps or visitors, effectively constricting such access to a need-to basis, as well as watching over who enters a company's premises. The latter information is usually combined with keeping logs about who entered through which company entrance using a badge.

- Visible security: Corporate Security is probably the most visible form of security in a company. Openly allying Information Security with Corporate Security therefore brings a clearly visible image (e.g. that of a Corporate Security guard wearing a uniform) of severity to the mind of employees when they think of Information Security. Also, it reminds them of the possible consequences for violating the Information Security policy (Corporate Security usually has a direct line to the corresponding law enforcement agencies). One way to achieve this effect is to get Information Security material published by Corporate Security officers, e.g. let them put up posters, install signs to label restricted areas etc.

- Security patrols: One of Corporate Security's tasks is nightly patrols through the company's premises to see if everything is as it should be. By raising Corporate Security's awareness of Information Security matters, Corporate Security officers can report any relevant matters they encounter during their night shifts to Information Security.

5.3.12 Facilities

A company's Facilities department can support Information Security in a number of ways, some of them being:

- Measures against natural catastrophes: The installation of smoke and water detectors is an integral part of protecting a company's information assets and therefore a part of Information Security. These detectors are usually installed by Facilities.

- Disposal of data carriers: 'Dumpster diving' is a jargon term for a method in which Social Engineers rummage through a company's garbage in order to find valuable information. Being perfectly legal (no one can be arrested for going through another person's garbage, as long this happens on public grounds), this method can be practiced very successfully with companies where the value of information has not been communicated sufficiently to its employees. Without such general awareness or a specific awareness of the practice of dumpster diving, employees may discard valuable information by simply throwing it into the paper trash along with everything else, effectively inviting a dumpster diver to discover and make use of it.

  Knowing this, the Facilities department can make it a habit to watch out for any data carriers such as CDs, DVDs or any suspicious-looking print-outs that have been discarded into an office's garbage can. These data carriers should be disposed properly, i.e. print-outs should be shredded, CDs and DVDs should be collected and stored securely until they can be transported to their eventual destruction so that no data can be retrieved from them.

- Installation of security enhancements: If not outsourced to another company, the installation of security enhancements such as a video surveillance system, additional badge access readers, etc. may also be handled by the Facilities department.

5.3.13 Graphic Arts Department

The Graphic Arts department can help Information Security by:

- Designing an Information Security logo that is easy recognizable and may be used in all materials concerning Information Security.
- Designing an Information Security web page: In some cases the company's Web masters are members of this department. If they are, they can be tasked with designing an Information Security web page. This can be done in cooperation with Application development, which could then take over the programming part.
- Design of posters, flyers etc.
- The development of short comic strips to emphasize a point in Information Security.

In addition, this department usually knows about the costs of publications and has contacts to outside companies that provide the necessary services.

5.4 Developing Leadership and Networking Capabilities

The accomplishment of successfully implementing Information Security policies relies first and foremost upon people's recognition and awareness of the importance of establishing and maintaining Information Security in the first place. This not only requires people's recognition and respect of one's abilities to conduct such an implementation, but also the development of a certain extent of leadership and networking capabilities. Especially the latter helps in becoming *the* go-to person, not only in all matters related to Information Security, but in some others as well. The following subsections discuss strategies that can help achieve this within a company.

5.4.1 Becoming an 'expert of experts'

The importance of making allies throughout the company has already been pointed out on numerous occasions in this thesis. In the early reconnaissance phase of implementing Information Security policies, interviews are not the only thing to be done. In addition, one also talks to different people from many departments, preferably in a relaxed atmosphere, the get a first-hand impression of their status and views on Information Security. Besides obtaining such information, this is clearly a networking opportunity in which one represents the Information Security department, giving it a face and a name to go to for any issues related to Information Security. While this partly serves to advertise one's cause, i.e. Information Security, it is also a good way of identifying all the experts in different areas of expertise that one might come in contact with during the implementation process. Besides information gathering and self-presentation, the goal of networking is therefore to become an 'expert on experts'. This helps in that one becomes an attractive choice for anyone inside the company for advice, not because one has the necessary know-how to give practical advice on any given subject, but because one can likely refer the most qualified expert and bring the right people from different departments together to find the best solutions – while watching closely if these solutions are Information Security compliant.

Also, by surrounding oneself with experts, one comes into close contact with their operations, making it easier to think about the ways and possibilities that Information Security measures can be implemented into these operations while causing as little disturbance as possible. Moving among these people (some of them may also be hidden opinion leaders), relying on the established status of experts they have earned during their time at the company, may lead others to perceive one as one of those experts as well, even if there has not yet been a chance to prove that. Also, more importantly, it provides these experts with a close contact in all matters of Information Security so that nothing that happens in their department in this regard will come as a surprise to them. Being in touch and being kept informed is something they will highly appreciate, benefiting these relationships.

The resulting network of experts should not be confined to one's company, as one should also seek out experts across a company's borders and, indeed, throughout the industry. The bigger the network, the better its advantages. Attending Information Security events such as

conferences or vendor presentations for new Information Security tools should present sufficient ways to get to know other Information Security professionals.

5.4.2 Developing leadership through training

There is good reason why Information Security training of employees should only be outsourced to another company if absolutely no resources are available for the Information Security department to conduct the training itself. By handing over this responsibility to an external trainer, one is denied the positive side-effect of other colleagues experiencing one as a trainer in one's area of expertise. Since the success of Information Security and the respect by colleagues that potentially accompanies it usually manifests itself in the absence of incidents, there is almost no better way to demonstrate one's competence and leadership capabilities in the field of Information Security than by training them. This also has the advantage of bringing the Information Security department closer to the employees of a company, showing them not only the people whose goal it is to make the handling of information assets more secure (i.e. the members of the Information Security department), but making the topic of Information Security something personal (which is one of the major goals of the training) rather than something anonymous taught by someone who is not even a part of the company (i.e. an external trainer).

The following chapter provides some insight into key aspects of proper Information Security training. Further aspects of good leadership practices in IT security are described in Whitman, Mattord (2007 [2004]: 10f).

5.5 Training

Overcoming apathy is one's greatest challenge in maintaining a constantly high level of employee awareness regarding Information Security. No matter how well trained employees become, as time passes they will become used to established processes, resulting in a drop of awareness. This negative trend can only be countered by regularly repeated trainings in matters of Information Security. The challenges that present themselves lie in maintaining the interest of trainees during training sessions as well as motivating them to learn and repeat important facts about the subject at hand.

Besides the question of whether to partly or entirely outsource training responsibilities to another company or to let the Information Security department perform the trainings itself (bearing in mind the advantages and disadvantages of both approaches as discussed), several other aspects need to be considered before devising an effective training program, with the goal of maximizing awareness as well as maintaining its level through repeated training sessions.

5.5.1 Training methods and tools

Training, in a case like Information Security, is more about refreshing the knowledge and awareness of the trainees than it is about presenting new content. Although technical advances make Information Security a field of constant change with respect to the challenges it has to face, its basic principles, e.g. the value of information, remain unchanged. The challenge in this is to refresh these principles without boring the trainees with content that has been covered a number of times before in previous training sessions, making the whole session appear useless and a waste of time. The solution to this is the use of suitable training methods and of any tools necessary to create variety in the way the content is delivered. What follows is a list of some of these methods and tools. Depending on the type of training being face-to-face, online or self-training, not all of these methods and tools are applicable for every training session. This list is simply an overall overview of how to create variety in Information Security training for trainees.

- Face-to-face presentations: The most traditional method of teaching also holds the greatest risk of trainees dozing off due to their own inactivity during the session, doing nothing but watching the presentation. To avoid this, such presentations should be as interactive as possible, using any means available to achieve this (multi-media presentations, open rounds for questions, group tasks and presentations etc.)

- Online multiple-choice tests: This method is especially useful for evaluating an employee's level of knowledge on Information Security. It allows a trainee to perform the test at his or her time of choice (within a specified time frame) and in a relatively short amount of time, depending on the knowledge of the trainee. This has the advantage of not boring those employees who remember the contents of the last training session, which are being tested, relatively well and at the same time giving them the chance to prove so in a simple way without much effort or taking long. Others, however, who do not pass the test, will be made aware of this and, after finishing the test, be given access to more detailed materials on those areas in which they failed the test or be told to re-visit a corresponding training session.

  What is more, these tests can be part of a training system which can store the test results of employees, count the times they attended to a training and, if it has been too long since the last time, inform them that they should refresh their knowledge or at least prove (by taking a test) that they do not need to. Automated training invitations may be sent through this application in such a case or if an employee has not taken a test after having been invited, but such an application also allows the collection of statistical data (more on this in chapter 5.6.6).

- Role-playing scenarios: Many matters of Information Security concern the exchange of information assets between people. Correct behavior in such situations can be trained through the use of role-playing scenarios, demonstrating the dangers that one might encounter during such exchanges (e.g. dealing with a Social Engineer, shoulder surfing etc.).

- Video training: This is obviously well suited for self- or online-training, depending on the way that the video material is distributed. Common ways of distribution are video CDs, DVDs or video streaming. Although the latter is becoming more and more popular today, one should consider the impact on the network infrastructure of a company in terms of the bandwidth that will be used if a great number of employees use video streaming simultaneously. Prior notice of the use of video streaming should therefore be given to the responsible department (likely Information Systems) so that arrangements for the temporary allocation of higher bandwidth capabilities can be made. These arrangements will be temporary only, because the simultaneous streaming of a particular set of videos only happens because of an actual training taking place during a specific time frame, during which many employees require a higher amount of bandwidth than usual because of video streaming. Even if the video material remains online (which it should, so that employees can also access it after a training session), bandwidth usage after the official training sessions can be expected to be much lower, as fewer employees will then access the video material simultaneously. However, at any time that video streaming needs to be used again, the corresponding department needs to be notified accordingly.

  The production of the video material itself should best be outsourced to a company specialized in these matters. There also exist pre-produced video materials on certain topics, among them Information Security. If these sufficiently cover one's training content, there is no reason to produce custom video training materials, as this naturally results in much higher costs than buying pre-produced materials. If they do not, however, individual material should definitely be produced, rather than rearranging the training material to fit the video material.

  Producing one's own material, provided that sufficient budget exists, is in any case the best solution, as one can also insert certain familiar aspects into the videos, such as the company's building, the Information Security logo etc. Also, this gives one the great opportunity to begin the video with a personal video greeting message by the company's CEO in which he or she addresses the employees directly and emphasizes the importance of Information Security for the company.

  If for some reason the use of video material is not possible, the next best alternative is multimedia presentations using standard presentation software such as Microsoft Powerpoint. This should, however, only be used if there is absolutely no way to acquire video material, because it is not nearly as effective in this context as videos are.

- Practical workshops: Workshops are very efficient in demonstrating the value of Information Security to employees by showing them some of the ways it may affect them in a very personal way. One way to do so is to announce practical workshops called, e.g., 'bring in your computer', where employees can bring their home computers or laptops to the Information Security department which checks them for software security measures (personal firewall, antivirus software, anti spyware

software etc.) and takes the necessary steps, when required, to make them secure. Some aspects of Information Security and network security, like cracking of weak passwords, cryptography, trojan horses, Wifi sniffing and hacking etc. can thus be demonstrated right in front of employees by using specially prepared computers (so as not to endanger any of the employee's private computers).

Through the practical nature of topics that may be presented during such workshops, the number of possibilities for such presentations is limited. After all, Information Security covers a much broader field than just the sum of these mostly technical topics. Nevertheless, the impact of such demonstrations and employees' realization of how this can personally affect them can, besides automatically raising awareness, greatly improve employees' attitude and respect for the work of the Information Security department.

5.5.2 Regular employee tests

One way to maintain the necessary high level of employee awareness of Information Security matters is by regularly letting employees take an appropriate test. This test should be multiple-choice and best be part of a training system that is capable of saving profiles for employees containing information such as:

- Last time the employee took an Information Security test
- History of each employee's test scores
- Number of repetitions an employee had to take after not passing a test
- Learning materials accessed by the employee as preparation for the test
- Number of reminders for taking a test

Every employee should take such a test at least every two years. Beginning with the last time he or she took the test, the training system should automatically send out a test invitation to that employee, informing of the necessity to take the test so as to allow him/her sufficient time for study while also providing useful links to resources that will help prepare for the test. Employees should be obligated to respond to this invitation, presented with the choice of either agreeing to take the test at the appointed date and time or postponing it while giving a reason for doing so. The latter will be passed on in a message to their supervisor, informing him or her that the employee in question has to postpone an upcoming test for the specified reason. This measure assures that employees take these tests seriously, as supervisors should see to it that their employees postpone these tests no more than two or three times. Also, once an employee has agreed to take the test, the training system should remind him/her of the test date, e.g. one week before the day of the test.

Failing these tests should invariably result in an invitation to training sessions, covering the relevant Information Security topics in which the employee did not achieve the score necessary to pass the test. These training sessions should be open to anyone interested in participating, yet are mandatory in case of employees who failed their repeated/regular test. Invitations to these training sessions, like the invitations to take the tests, need to be either

confirmed or postponed for a specific reason by the employee. Non-attendance of these training sessions needs to be sanctioned unless the absence is permitted by the employee's supervisor who may give permission to postpone the training under certain circumstances. After completion of the training, the employee may retake the test, yet should also be informed that the number of times that he or she repeats the test will be forwarded to his or her supervisor in case it exceeds a certain number of repetitions (e.g. three times).

5.5.3 Special training

In case of certain events (e.g. an exploit in a software that the company is using), special training sessions may be organized. Attendees may be employees from specific departments or, if the event affects the whole company, all employees. These stand-alone trainings should end with taking a small test about the content that has been covered in that session.

Invitations, tests and participation control for these trainings should be handled as described in the preceding section.

5.5.4 Orientation days

For Information Security, Orientation days are special in that they are more than simply training events. This is likely the first time that employees that start working at a company come into contact with the company's Information Security policy, e.g. its views on Information Security and what is expected of them in this regard. A number of aspects need therefore be addressed on Orientation days:

Employee handbook: Every employee should be given a welcome package containing all the information he or she requires. Part of this package is likely an employee handbook created by HR. While this handbook contains useful information for new employees, including details on what he or she requires for a better understanding of the way Information Security is handled at the company, the Information Security policy statement should not be part of this employee handbook, but only be referenced in these materials. In other words, it should be kept separate from the employee handbook and presented on a separate extra sheet to underline its importance. Moreover, any other relevant Information Security materials (standards, procedures etc.) should be referenced in this handbook so that employees know they will come into contact with them sooner or later, along with information on how to access these materials (they should easily be available through the Information Security web page, which should be accessible through the company's Intranet web page).
Any materials written for Orientation days should be written with the same principles (simplicity etc.) that apply to the process of writing Information Security policy documents and be kept well up-to-date. They should be written with all the seriousness required, yet should not create a threatening impression. Also, any Information Security materials, whether they are part of the employee handbook or not, should contain the Information Security department's logo. If they are, one should read the entire handbook to make sure that the Information Security part fits with the rest of its content.

Information Security agreement: At some point during Orientation days, the time comes for the mandatory signing of an Information Security agreement, i.e. the legal commitment of an employee to adhere the company's Information Security policies along with a confirmation of knowing about the consequences of failing to do so. This agreement should adhere to the following principles:

- It should consist of a number of simple statements, each starting with "I"
- If possible, these statements should be written so as to convey a personal meaning to the employee
- It should be easy to understand, so that violations are easily recognized
- Consequences of such violations should be clearly outlined
- Signing of this agreement should best be done on paper, as this conveys the strongest impact on people's perception in terms of its importance (i.e., it should feel like signing a contract). Another option is to have the agreement online and sign it by pressing a button.
- HR can keep a record of the signing date and require employees to renew their signature on that agreement every two years.

The following page shows an example taken from Desman (2002 [2001]) that illustrates what an Information Security agreement may look like.

Information Security Agreement

In accordance with the information security policies, standards and procedures of the ABC Company, I, the undersigned do fully agree with each of the below noted points:

6. I have been given a copy of the ABC Company information security policy.
6. I understand that there are specific standards and procedures for the handling of ABC Company information assets and have been informed as to how to review them. I will do so before any attempt to utilize those information assets.
6. I know that I will be issued specific access capability to ABC Company systems and will not attempt to expand upon that access. I will use all information assets as intended by the company.
6. I will keep any user IDs and passwords issued to me in full confidentiality and will not share them.
6. I will either lock or log off any terminal that I am using when I leave that position.
6. I will not discuss ABC Company proprietary information with anyone.
6. I will make certain that waste materials that contain ABC Company confidential information are destroyed and not included with common trash.
6. I will conduct myself in a manner so as not to place any ABC information assets or the systems upon which they reside in peril of destruction, contamination, compromise, or loss.
6. If I detect the misuse of ABC Company information assets by other parties, I will inform my supervisor immediately.
6. I understand that failure to comply with any of these points could lead to disciplinary action up to and including termination and prosecution.

I have read, understand, and agree with all of the statements made above.

(Signed) _____

Employee printed name _____

Date _____

Witness_____

Fig. 7: Example for Information Security agreement for company ABC (Desman, 2002 [2001]: 79)

Presentations on Orientation days: Orientation days are filled with numerous presentations, so the time to communicate one's message about Information Security will likely be short. As this is all the more reason to make the most of this time, the following points should help in doing so:

- Presentation mediums: One's presentation should be tailored to the mediums that are available during Orientation days' presentations. Availability and functionality of these mediums should be verified before the presentations.

- Introduction: A good way to introduce the topic of Information Security on Orientation days is to have the company's CEO give a statement about its importance for the company, demonstrating top-down support of Information Security within the company. If the CEO can not appear in person, a video introduction will suffice (similar to the one used during video trainings).

- Content: The core of one's presentation should be the company's Information Security policy statement, as this presents the company's view on Information Security in

condensed form. In doing so, brief reference should be made to the basics of Information Security, such as the value of information, rules for the use of communications media, passwords etc., depending on the amount of time available for the presentation. For topics that can not be covered in sufficient depth, further reading materials should at least be referenced. One should also keep a record of these topics, so as to optimize the presentation for the future.

A good approach to find the content for such a presentation is by keeping an outline of the content that one wishes to cover. The following presents a sample outline for such a presentation.

I. Introduction
   a) Presentation of oneself and what one represents (e.g. the department of Information Security)
   b) The reason for having this presentation
   c) What will be covered
II. Introduction to company policy
   a) Presentation of Information Security policy statement on a single slide
   b) Going through all the statements
III. Information assets and the value of information
   a) Presentation of a solid, memorable statement on how the company considers information and its processing environment a corporate asset.
   b) Classifications of information
      1. Definitions of the levels of sensitivity in the company
      2. Examples of each level
      3. Short oral quiz: Presentation of information examples to audience, get input on the presented classifications
      4. Explanation of how divulging any of the more confidential assets can harm the company
IV. Handling of information
   a) Where it is stored
   b) Backups and recovery
   c) What to do with outdated information
   d) What employees are expected to do
V. Viruses
   a) What they are
   b) Where they come from
   c) What to do about them
   d) What to watch out for
   e) Hoax vs. real threat
VI. E-mail
   a) What is allowed and what is not
   b) Confidentiality in E-mail
   c) Malicious attachments

d) Taking care of one's mailbox
e) Consequences of misuse

VII. Voice mail
a) Weaknesses
b) Proper usage
c) Housekeeping
d) Types of incursions

VIII. Verbal communications
a) Telephones
b) Public places
c) Interactions with friends and family

IX. Personal responsibility
a) Review of previous
b) What wrong looks like
c) What to do
d) Who to call

X. Important phone numbers and E-mail addresses
a) Information Security department
b) Corporate Security
c) Help Desk
d) Human Resources
e) E-mail postmaster
f) Others

XI. Conclusion
a) What the audience's contribution to learning about Information Security means to the company
b) What the audience's performance means to the company
c) What the company's profitability means to the audience and how it affects them
d) Short quiz about the covered content of the entire presentation

Fig. 7: Example for Information Security presentation outline for Orientation days (based on Desman, 2002 [2001]: 137)

Again, depending on the time available, certain points of such an outline may not be covered during the presentation, but should at least be referred to.

- Interactive presentations: Naturally, each presentation consists of a presenter and an audience. As has already been mentioned, this constellation can lead to an uneventful, even boring experience for the audience. In order to avoid this, there are various ways of creating interactivity in such presentations, such as asking direct questions to the audience and letting them shout the answers out loud. Whether these spontaneous responses are correct or not, this technique has two effects: the message that is communicated by the presenter will more likely be remembered this way and the audience will remain more attentive during the presentation.

- Speaking in statements: Another way to ensure that the audience remembers the contents of one's presentations is speaking in easily memorable statements.

- Questions: One should constantly read the audience for reactions based on their expressions and body language. Frequently, questions that need answers are not asked because of shyness or fear of embarrassment before others. One should make clear that there is room for all questions, but that, due to keeping a timeline, questions that require more discussion should best be left for after the presentation. One also needs to recognize that if multiple questions are being asked about one specific topic, one's presentation has likely not sufficiently covered this topic and probably needs a corrective review.

- Success stories: The importance of presenting oneself as an expert in the field of Information Security and to show leadership capabilities right from the start (i.e. beginning with Orientation days), has already been pointed out. Success stories about past events or incidents, if included in a presentation, help to create that image with the audience, but they also add to a more relaxed, collegial atmosphere during the presentations.

- Personal attendance in case of a substitute presenter: In some cases an Orientation day presentations may not be given by oneself. In such a case one should nevertheless, from time to time (at least every two years), attend such presentations as part of the audience in order to see how the presentations go, if one's content is conveyed as intended, and check the response by the audience. This is also a chance to give feedback to the presenter after the presentation and, in later presentations, see if this feedback has been heeded by the presenter.

- Time slot in Orientation day presentations: Information Security presentations should best take place on the first day of Orientation days. If nothing else, one should negotiate with HR in order to be allowed at least a short presentation of the company's Information Security policy statement on the first day, with another, more substantial presentation following up on another day.

5.6 Getting the budget for Information Security measures

In some cases, very valid ideas for Information Security measures, using sophisticated methods and tools, have not found their way into actual implementation, because their usage was deemed too costly by the managers responsible for the allocation of Information Security budget. Even while doing the best one can with the resources available, such a situation can leave an Information Security department with simply too little to protect a company's information assets sufficiently.

The process of budget allocation has always been a challenge for security, regardless of its field of operation. Information Security, being an area of security that works less with the implementation of purely technical solutions, but focuses more on process optimization and changing people's behavior, requires not only constant attention, but also continuous optimization in matters of training, user awareness as well as the use of state-of-the-art technical solutions. All of this, however, also requires budget. Yet the fact that successes in the field of Information Security define themselves by the absence of incidents makes discussions over budget with the responsible management a challenging issue (to say the least), which hinges on presenting the right facts in the right way with the right strategy in mind. Some of the ideas for doing so, which are presented in the following pages, have already been discussed fully at some point throughout this thesis and will therefore only be referred to here in order to underline their importance in the process of budget remittance. Others, however, will be elaborated with more detail, especially the ways of evaluating Information Security performance in facts and numbers and giving effective presentations to management and other departments involved in Information Security measures one is trying to get a budget for.

More than a mere list, this section is about combining these ideas into a strategy to obtain the necessary budget for a company's continuous Information Security program.

5.6.1 Getting support from others

There is arguably no context in which is the support of others has more importance than in budget negotiations with management. Since this aspect has already been elaborated in detail, only a brief summary of the parties one should best have support from during budget negotiations is provided here:

- Allies in other departments: Not necessarily only those that will be affected by the project or measures that one requires budget for, but any who may say something in favor.

- (Hidden) opinion leaders: Obviously, as described in the corresponding sections (most notably, section 4.4.1), their support is of great importance.

- Experts: Not only inside the company, but also outside of it, e.g. other Information Security contacts, contacts at a university department specialized in what the project/measures in question are about etc.

- Supervisors: They have experience in negotiations of this kind. One should keep in close contact with them, letting them know that what one is trying to accomplish is not the work and responsibility of a single and isolated department (Information Security).

- Internal auditors: As described in the corresponding sections (most notably, section 4.4.1 and 5.3.6).

- External auditors (if available): These may be harder to come by, yet their support is all the more valuable.

If possible, representatives of these parties should be present during the negotiations to voice their support if and when given the opportunity to do so. This can also happen in written form (e.g. an E-mail to management recommending the implementation of the project in question).

5.6.2 Addressing open audit issues

Open audit issues, especially if they were the result of an external audit, receive considerable attention and high priority by management. If they are clearly Information Security-related and identified as such by the auditor's report, getting the budget for measures intended to close such issues is usually no problem, as proposals for closing an open audit issue are usually welcomed by management. However, even if they are not Information Security-related, there are still ways to use open audit issues to the advantage of one's Information Security agenda.

To do that, one should know about the issues that have been found during an audit and identify in them a possible connection to Information Security. If such a connection can be found, one should look up the corresponding departments in which the audit issues have been discovered and discuss ways to join resources and efforts in closing these issues, while – under the safe cover of closing an audit issue – addressing one's Information Security agenda along the way.

5.6.3 Using past or recent Information Security incidents

Past or recent Information Security incidents, whether they occurred at another company or one's own, usually make persuasive arguments for the implementation of further Information Security measures and, by implication, for the necessary budget to do so.

The presentation of such incidents with the aim of supporting one's request for budget for further Information Security measures has already been elaborated in some detail (section 4.4.2). The present section points to the most relevant points and questions to ask in order to use such incidents to one's advantage.

External incidents:

- Information gathering:
    - Where did the incident occur?
    - Was there more than one incident or was more than one company affected (e.g. with the Melissa virus outbreak)?
    - What relations are there between the victim(s) and one's own company?
    - What were the consequences for the victim (loss of customers, stock market, monetary, contracts, reputation)? Are there any concrete numbers on these losses (which would be valuable, but usually hard to obtain)?

    - No names (none are required) or exposing of others.

- Critical question:
    - How would one's own company have reacted? Would it have fallen victim to the incident as well?
        - No: Why not?
            - Presentation of effective Information Security measures currently in place at one's company, proving that the budget spent so far has been spent well.
            - Giving credit to anyone that has contributed to this.
            - This is no reason to rest on one's laurels: **Continuous vigilance requires budget. Presentation of the requirement for budget to maintain that level of efficiency in protecting a company's information assets.**
        - Yes: Why?
            - Presentation of room for improvement in the company's current state of Information Security. **This requires budget.**
            - Dramatic declaration: Under the current circumstances, one's company would suffer the same fate. So far it has been sheer luck that nothing has happened, but this can change rapidly.
            - Information Security is not a matter left to coincidence; after presenting the fate of the victim company, this should have become clear to everyone in the audience.

Internal incidents:

- Information gathering:
    - What was the damage? What has been lost?
    - Did other companies suffer the same fate?
        - Yes
            - Can we learn from them or each other?
            - Consult with other Information Security professionals, if they are available.
        - No
            - What did others do better?
            - Consult with other Information Security professionals, if they are available.

- Critical question:
    - Could this have been prevented?
        - Yes (obviously): How?
            - Was the problem known before the incident, yet not addressed?
            - If so: Why not? **No budget?**

        - If not: There is obviously room for improvement. **This requires budget.**
    - No:
        - This is an answer that is neither acceptable to any manager, nor useful for one's undertaking of getting more budget for Information Security.
        - The answer should therefore always be 'yes'.

5.6.4. Effective presentations

There are numerous factors that contribute to a successful presentation and will convince the audience of one's viewpoint. In Information Security, such convincing, if strong enough, can go along with management's granting of budget for the implementation of Information Security measures that are vital to the protection of a company's information assets.

Presented below are some of the factors which are particularly relevant for presentations for Information Security projects. Each of them can help in presenting a convincing argument to management and gain the required budget.

Gain-based vs. fear-based approach:

Getting approval for an Information Security project (i.e. for the required budget) is a matter of convincing management of the necessity of its implementation in two ways:

- Gain-based: By presenting the gains to the company once the project has been implemented

- Fear-based: By presenting the (potential) losses to the company if the project is not implemented and the chances of this happening

Although successful interpersonal communication is usually based on a positive emphasis, the fear-based approach is usually more convincing in matters of Information Security. The reason for this lies in the emphasis that the status quo has for management. The gain-based approach may lead to considerations about the gains a project would bring compared to the status quo, but also possibly to the conclusion that one's performance has been satisfactory so far. This might well be taken to mean that there is no need for the project in question, at least not at the moment, and that budget should be spent elsewhere instead.

The fear-based approach, on the other hand, leaves an evaluation of the status-quo unsatisfactory, as there is the constant danger of losses to the company due to incidents. If the project in question is presented as a solution to an ever-present danger, this will appear more attractive in the eyes of management, as it provides stabilization of the status quo, especially if this danger is presented in a dramatic way.

A good presentation should combine both approaches: first, the fear-based approach in order to create a feeling of absence in the status quo, of something that the project in question would provide if implemented. Then one should follow up with a gain-based approach to emphasize not only this provision, but additional benefits to the company by the implementation of the Information Security project in question.

Picking up 'action items': The term 'action item' is used in this thesis to describe a word that is unconsciously used frequently by one person in its conversations about a certain topic, manifesting its importance to this person. Picking up on these 'action items' and using them in a certain context during a conversation is a persuasion technique that can also be used in discussions or presentations about Information Security projects. If, for instance, a manager used the words 'stability' and 'reliability' of information systems multiple times during interviews, one should, during one's own presentations, use these exact terms – no descriptions or synonyms – as their multiple use conveys importance of these terms for this particular person. This gives the audience the impression of having been understood and 'giving them what they want', which is naturally something they will welcome greatly.

A powerful way to do that in the context in question is during multiple presentations. Especially larger projects will not be granted permission for implementation based on only one presentation. Where many departments are involved, many issues may come up, so there may be need to go back to the drawing board and come back with a better solution than the one presented the first time. If during a presentation one is asked questions or receives feedback from the audience about certain topics in which 'action items' are used and is asked to come back with a more developed approach for a project, one can then specifically use these 'action items' while addressing the audience during the next presentation. This creates a positive feeling with the audience, ideally a feeling that their feedback has been followed or that answers have been found to questions that were asked before. This technique is called 'consensus management'.

Responses to feedback should be given not only during upcoming presentations, but also beforehand via E-mail to the corresponding person or department. The reason for this is the ability to set a timeframe for the acceptance of the solution given to the original feedback that has been given by this department, making it possible to get a modified, improved response to this feedback ready for the next presentation.

Focus on strengths, reframe weaknesses: Obviously, one should present one's work in the best possible light. Therefore, any successes in the past, especially if clearly based on the past implementations of projects, should be mentioned to show management that the budget spent so far has been used wisely and to the full advantage of the company.

Any weaknesses (resulting in incidents which had a negative impact on the company's information assets) should be reframed if possible. Incidents that have happened because of these weaknesses should be presented as having happened because not everything was done that would be necessary to sufficiently secure a company's information assets. As this leaves open the question what can be done to improve this in the future, one should have answers

ready in the form of concrete project plans, requiring only management's call to grant the budget necessary for their implementation.

Simple, recognizable, repeated bottom lines: A good presentation practice is to create a few simple, yet easily recognizable bottom lines that are repeated throughout the presentation. This will make them easier to remember for the audience and give the content of the presentation a clear direction as to what needs to be done. These bottom lines should, if possible, contain 'action items' that have been identified beforehand.

Questions and answers: Obviously, one should prepare for a presentation as well as possible and try to answer any questions that may be asked by the audience. Since it is not possible to prepare for any and all possible questions in advance, a good way to deal with questions to which one has no answer is to promise that one will be back with an answer soon. This should be taken literally, as especially the timeframe that it takes for one to come up with an answer will be critically judged by the audience. If one presents a satisfying answer quickly, this shows enthusiasm. This is not only a good impression to give, but also something that may easily catch on to others.

Management summaries: Each presentation should be followed by a summary of what has been discussed and what conclusion have been taken or if the subject has been left unresolved and will be addressed again. This summary should especially address management, but similar summaries should also be sent to all parties present during a presentation, focusing on their participation on the project in question.

These summaries should follow up quickly after a presentation and should be written with the help of the Documentation department.

5.6.5 Showing successes

Due to the dilemma of having its successes defined primarily by the absence of incidents, Information Security constantly faces the need to justify its existence to a company's employees and to management. With respect to a company's employees this means demonstrating that Information Security serves the protection of a company's information assets and securing operations in which all employees are involved. To management, in many cases, this means simply that the budget spent on Information Security was money well spent. As put by Mark B. Desman, "Successes create credibility and credibility reassures management that you are going about it the right way." (Desman, 2002 [2001]: 184)

Distribution channels: Information Security is a subject that requires constant publicity and advertising. Thanks to the allies one has made, this should happen by making use of all the information distribution channels that are at one's disposal.

To demonstrate the well-established position of Information Security within a company, the cooperation of the Information Security department with other departments of a company and to ensure their support, it is imperative to share credit for Information Security successes

where it is due. This gives success messages publicized through the information distribution channels an even greater impact, as these topics are not being seen as relevant only in regard to the Information Security department, but to the operations of other departments as well.

What content to publish: Simply everything that is positive in regard to Information Security and that can be put into impressive words with the help of the Documentation department. Examples are:

- Successful responses to virus outbreaks, giving credit to the virus response team.
- Regular summary messages about Information Security-relevant facts (examples will be presented in the upcoming section), sent out e.g. every three months.
- Successful implementation of new Information Security measures, giving credit to all departments involved.
- Upcoming introduction of new Information Security measures (advertising).

The overall idea is to show the company that Information Security is alive and working for them.

5.6.6 Evaluating Information Security performance

There are two reasons for the evaluation of Information Security performance:

Performance meetings: From time to time (at least once a year), there will be a call for a performance meeting to evaluate the performance of the Information Security department and the measures that have been implemented place by it. In these meetings the performance of these measures will be discussed between

- *management* which, based on this performance, assesses if these measures have produced the desired outcome or not,

- the *Information Security department* justifying its existence and the budget spent on Information Security measures in the past, so as to assure budget for the future, and

- the *departments that are involved in these measures* and, hopefully, support the Information Security department.

This evaluation usually goes hand in hand with deciding whether to continue with these measures, terminate or extend them. This direct relation to the allocation of budget makes performance meetings a delicate matter for the Information Security department, which is all the more reason to attend them well-prepared.

Throughout the year, advertising the necessity of Information Security measures may be enough. During yearly performance meetings, however, management usually expects to see

hard facts, i.e. numbers and statistics, informing about the performance of the measures that budget was spent on during the last year.

Obviously, not all of the factors that make the implementation of Information Security policies a success can be expressed in numbers, especially because this success is mostly based on the absence of incidents. There are, however, some factors that can be considered in comparison to the time before the current Information Security policies were implemented, highlighting the improvements of the present policies.

- The number of Information Security-related errors and incidents that occurred at the company
- The number of break-ins that the company could register (this number can be provided by the department responsible for network monitoring, likely Information Systems).
- The number of open audit issues that have been closed
- The number of times that an employee terminal has logged off automatically (the less, the better; this is an indicator of employee awareness about not leaving their terminal without logging off)
- The number of times an employee password was rejected at a time when the password needed to be changed because it was not strong enough (the fewer, the better, showing employees' awareness about proper password design)
- The uptime of critical systems in spite of incidents (virus outbreak, denial-of-service attack)
    - Has something happened?
    - If so, how?
    - How long was the system out?
    - How often has this happened?
- Incident recovering and lessons learnt
    - What has changed since specific incidents occurred (concrete measures)?
    - Have similar incidents occurred since then?
- Education and training (data provided by training system)
    - Number of regular tests taken
        - Percentage of tests passed
            - Percentage of tests passed on first attempt
            - Percentage of tests passed after repetition
        - Percentage of tests failed
            - Percentage of employees in repeated training
    - Percentage of employee attendance of Orientation days training
    - Percentage of voluntary employee attendance to training
    - Hits on Information Security web page
    - Hits on Information Security-related links
- Number of Information Security-related questions asked by employees
- Statistics collected on given new threats, sources are e.g. Gartner, SANS, SAFER, CSI, ISSA (Desman, 2002 [2001]: 191)

In this, one should also be on the lookout for trends. If a positive trend is recognizable, this is a clear success of one's efforts. Nevertheless, one should never neglect keeping up-to-date on current Information Security threats (e.g. using statistics obtained by the organizations mentioned above), so as to be prepared for what the future might hold in store.

Personal feedback: Aside from budget negotiations, all of the above factors also serve as a personal indication of one's success. Depending on the outcome of that personal evaluation (which may be quite different from the one presented to management in order to obtain budget for future Information Security projects), one may need to ask additional questions, such as:

- How can we enhance the above factors even further?
- Coverage
    - How many people did we reach approximately?
    - If we reached 60% (example), we must now focus on the other 40%
    - How do we achieve that?
- Audit reports
    - Do issues that have been found once resurface in subsequent reports?
    - What was one's reaction to the first discovery? Why did this not suffice?
- Future projects
    - Is now the best time to ask for budget for a particular project?
    - Who can I get to support it?
    - Who may be against it and why?
    - etc.

6. Conclusion and outlook

Implementing Information Security policies is not a simple task. During the process of implementation, one might even reach the surprising conclusion that the greatest challenges faced in Information Security have nothing to do with ill-meaning persons or criminals intending to steal a company's valuable information security assets, but with the very people whose information assets one is trying to protect through Information Security policies and measures. An adversarial approach, however, in which one tries to force Information Security onto employees, is sure to fail. Indeed, success in the implementation of Information Security policies and efficiency in their application can only come through working together, *with* a company's employees and within a company's culture, not against them.

This realization has its value, yet good will alone does not suffice, as the relationship between Information Security professionals and other employees is often tense. This stems from an unfortunate, but inevitable downside of Information Security: As a result of optimizing work processes in terms of Information Security, these processes become more complex than they were before. A natural and, up to a point, even understandable reaction to this fact is therefore that employees resist Information Security measures. Such resistance needs to be overcome, as the most significant asset in one's arsenal for protecting a company's information assets is the awareness of those very employees – awareness of the value of information, the threats that they face while handling information assets, and the need for Information Security, with all the implications this has for a company's business.

As if this were not enough of a challenge already, working in a field where success is defined through the absence of incidents, the Information Security department constantly needs to justify its existence in the eyes of management. Getting the budget to build and maintain an ongoing Information Security program, devising policies and conducting their implementation is another substantial challenge faced by the Information Security department of any given company.

Both of these challenges can only be overcome by accepting that the implementation of Information Security policies is, in fact, a sales matter in which one needs to sell Information Security principles and measures to the employees of a company (so that they will be followed by them) and its management (so that the necessary budget will be granted to implement these measures). This requires not only in-depth knowledge about one's company, its employees, management and culture, but persuasive strategies that can only work with the help of allies throughout the company. Such allies are thus necessary for their support of the principles of Information Security as a continuous process and to establish the necessity for Information Security policies within a company.

While technology-based challenges for Information Security become more advanced as time passes, so do the technical means to counter these challenges. The implementation of Information Security policies, however, remains a challenge that is and will remain primarily a people matter that requires corresponding approaches to solve it. While this thesis' goal was

to present such an approach, it must be acknowledged that such approaches may be as diverse as people's attitudes toward Information Security, making the further study of viable approaches for the implementation of Information Security policies a subject of continuing interest.

7. Bibliography

- Anderson, Ross (2001): *Security Engineering – A Guide to Building Dependable Distributed Systems*, Indianapolis: John Wiley & Sons
- Bundesamt für Sicherheit in der Informationstechnik Deutschland (03.07. 2010): *IT-Grundschutzhandbuch*, https://www.bsi.bund.de/cln_183/DE/Themen/ITGrundschutz/StartseiteITGrundschutz/startseiteitgrundschutz_node.html
- Bundeskanzleramt Österreich (04.06. 2010): *Österreichisches Informationssicherheitshandbuch v2.3*, http://www.a-sit.at/de/sicherheitsbegleitung/sicherheitshandbuch/
- Bundeskanzleramt Österreich (04.06. 2010): *Bundesgesetz über den Schutz personenbezogener Daten*, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597
- Bundeskanzleramt Österreich (04.06. 2010): *Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird*, http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849
- Denning, Dorothy E. (1999 [1998]): *Information Warfare and Security*, Upper Saddle River: Pearson Addison Wesley
- Desman, Mark B. (2002 [2001]): *Building an Information Security Awareness Program*, Boca Raton: CRC Press LLC
- International Standard Organisation, *ISO/IEC 27001:2005*, http://www.27001-online.com/iso-27001.htm
- Kersten Heinrich/Klett, Gerhard (2008 [2005]): *Der IT Security Manager*, Wiesbaden: Vieweg+Teubner
- Kurose, James F./Ross, Keith W. (2003 [2000]): *Computer Networking – A Top-Down Approach Featuring the Internet (International Edition),* Upper Saddle River: Pearson Addison Wesley
- McClure, Stuart/Scambray, Joel/Kurtz, Goerge (2005 [1999]): *Hacking Exposed 5th Edition*, Emeryville: Mcgraw-Hill Professional
- Mitnick, Kevin D. (2002): *The Art of Deception – Controlling the Human Element of Security*, Indianapolis: John Wiley & Sons
- Mitnick, Kevin D. (2006): *The Art of Intrusion – The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers*, Indianapolis: John Wiley & Sons
- Råman, Jari (2006): *Regulating Secure Software Development*, Rovaniemi: Lapland University Press
- Schneier, Bruce (2000): *Secrets and Lies – Digital Security in a Networked World*, Indianapolis: John Wiley & Sons
- Skoudis, Ed/Liston Tom (2006 [2001]): *Counter Hack reloaded*, Upper Saddle River: Prentice Hall

- Whitman, M. E./Mattord, H. J. (2008 [2004]): *Management of Information Security 2nd Edition*, Florence: Course Technology

universität wien

MASTERARBEIT
Abstract

Titel

Challenges in Implementing Information Security policies

Verfasser

Andreas Reichard

angestrebter akademischer Grad

Diplomingenieur

Wien, 2010

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienblatt:	Wirtschaftsinformatik
Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

1. Introduction

Every kind of information carries a specific value. The exact amount of that value depends on factors such as its content, confidentiality, and owner. In some cases, especially in business environments, this amount can be expressed as a monetary value; in other cases this is not possible. Consequently, the uncertainty about possible consequences of sensitive information getting into the wrong hands has led to extensive planning of ways to prevent this from ever happening. Dealing adequately with information – not only highly sensitive information, but information in general – in a way that does not constrain business processes unnecessarily, while still protecting the information as a valuable asset from illicit access, falls into the field of Information Security.

Recognizing the danger of information exposure, many businesses have invested considerable time and effort into the creation of an Information Security program. The creation of such a program is a complex task in its own right, worthy of recognition. The effort devoted to such a program, however, does not guarantee the efficiency of its implementation, i.e. the crucial issue of whether the people affected by it will also comply with it and, if they do, to what extent. Investing substantial effort into the design of an Information Security program without sufficiently acknowledging how coworkers will be affected will likely lead to a large gap between the conception and the application of such a program. In a worst case scenario, this may even render the entire Information Security program useless, if people do not recognize an overall benefit for their own work or for the company as a whole. On the contrary, if they see little or no benefit in compliance, accomplishing their day-to-day tasks in the most efficient and time-saving manner will receive the highest priority instead of Information Security. This usually involves violating a number of Information Security measures put into place to protect valuable information.

This thesis recognizes that there is a substantial difference between the *design* and the *implementation* of an Information Security program. It is that difference which is responsible for the existence of a possible gap between conception and application of an Information Security program. The question this thesis intends to answer is this how this gap between conception and application can be reduced or, more to the point, how Information Security can be communicated to people, employees and management alike, so as to make them recognize the overall value of Information Security – both for them personally and for the company they are working for. Only through such understanding, i.e. awareness, can compliance with an Information Security program be achieved, making it work as intended by its design.

Although the successful implementation of an Information Security program is closely related to its design and creation, it must be pointed out that this thesis is not focused on the *design* of such a program per se. Due to the nature of this close relation, this thesis may indeed offer additional insight into the design of an Information Security program. Its main topic, however, is overcoming any obstacles during the implementation phase that might appear during the application of an Information Security program and thereby reduce its effectiveness. Doing so will maximize the acceptance of an Information Security program on the part of the people affected by it because it is seen as an effort to protect information as a common asset.

2. The Value of Information

Every company has assets which are given a specific value. The loss of these assets represents a loss of value to the company that owns them. This loss becomes even greater if these assets are connected to the company in some specialized way. By that definition, a company's information is specialized in many ways. Different kinds of information can have different values for different individuals. For every kind of information there is someone for whom this information has value. This is true even for seemingly unlikely cases. As a consequence, every kind of information should be protected against unrightful access and possible exploitation.

Seemingly harmless information in the hands of a person who knows how to use it can still cause great damage to a company. So-called 'Social Engineers', by using linguistic and psychological methods, are specialized on extracting this kind of information from unsuspecting employees. This information can later be put to use to damage a company. Possible contexts in which these methods are being used are corporate espionage, blackmail and privately motivated enrichment, e.g. via identity theft.

Indeed, identity theft is one of the most wide-spread methods of application for stolen information today. Through the spread of online communities, e-commerce etc., many people have created for themselves a number of virtual identities. The reason for the existence of such virtual identities, from the perspective of an institution (e.g. a company offering to do e-commerce), is to have a representation of the identity's owner with whom it can communicate and do business with. This means that in the eyes of such an institution this identity *is* virtually the owner. Anything that is done via use of this virtual identity is traced back to its owner and deemed to have happened with his knowledge and compliance.

The growth rate of e-commerce over the Internet has proven that this concept has helped to open markets throughout the world, enabling companies and costumers to gain access to each other and do business. Unfortunately, this concept has also introduced a set of problems, a crucial one of them being the illegal use of a virtual identity by another person who is not the original owner of that identity. This is also known as 'identity theft'. This represents a problem insofar as, from the point of view of the institution handing out these identities, any action committed through the use of a virtual identity is seen as having been committed by the person to whom this identity is registered. Obtaining such a virtual identity by illegal means and using it for criminal activities is therefore one way to frame someone else (the original owner of the virtual identity) for actions that this person did not, in all actuality, commit, while most likely benefitting from it in some way.

The theft of a virtual identity is one of the most recent developments caused by the spread of the Internet access throughout the world. This problem, however, is not solely Internet-based. Where people are involved, there are numerous situations in which they themselves present their identities to others in order to gain access to restricted information (bank account numbers, pin numbers etc.). In every one of these situations, there exists the possibility of stealing the identity by which a person identifies itself to another person or institution and posing as the original owner of that identity. These cases are also considered identity theft, though not Internet-based, happening in the so-called 'real world'.

3. Information Security Policies

The value that one specific piece of information is given may be the result of a subjective decision made by one individual. Based on that decision, this information will be treated with a specific level of confidentiality by this individual and, possibly, passed to another. As such a subjective decision will vary from person to person, so does the level of confidentiality. In an environment where Information Security is taken seriously, such a large margin of variation is not acceptable. This necessitates a set of documents, rules and policies - which are written down in order to leave no doubt about how information is to be treated - that determine both the level of confidentiality and the people who shall have access to it. Such a set of documents is referred to as 'Information Security policies'. Importantly, these documents are not entirely static and are subject to regular review and change, should there be a need (e.g. because of changes in technology or management).

Information Security policies consist at least of the following parts (with more parts being added if the need arises):

- Policy statement
- Standards section
- Procedures
- Principles
- Guidelines
- Classifications (document confidentiality, access restrictions, incident classification)
- Definition of terms

Responsibilities concerning Information Security policies must be clearly defined within a business. These responsibilities include the establishment of Information Security policies, management, maintenance, review and updates, enforcement and adherence in cases of policy violations and legal prosecution. Documentation must also detail what life cycle policies have before they have to be reviewed, updated or even discarded to be replaced by a newer version.

The scope of Information Security policies depends on the size of the business it operates in and its business connections, probably extending to other countries. Information Security policies directed at only one business on its own are not sufficient if that business has partners which do not share its management's view on Information Security. Since these partners often have access to sensitive information which is protected by the Information Security policies of the company, their handling of this information may be in violation to the Information Security policies. This practically renders the Information Security policies useless as the point of vulnerability concerning Information Security has not been addressed by the Information Security policies: it has only been outsourced to a business partner who now represents a potential Information Security risk. It is therefore imperative that guidelines for the treatment of information within business partnerships are established in coherence with the relevant Information Security policies. Moreover, differences between national and international business partnerships need to be taken into account, partly because of different regulations that may exist in other countries.

In case those Information Security incidents occur, a functioning chain of reactions must take effect. This must necessarily include the classification of the incident, proper response and reporting. The response to an Information Security incident depends on the classification it

receives. These classifications as well as established response actions and other details must therefore exist as an integral part of any Information Security policies.

A vital part of Information Security policies' life cycle is the regular review and update, should one be necessary. This implies that the responsibility of keeping up to date with new threats to Information Security, recent Information Security incidents and new vendor offerings to counter these threats must be clearly defined. A good overview over these matters as well as the company's resources is necessary to create a realistic outlook on what may yet become a threat to the company and how it can be dealt with.

4. Challenges in establishing Information Security Policies

Implementing Information Security policies includes many measures that have to be taken, but also requires that the people affected by these measures must accept changes that will make their work life more complicated than it would normally be. The average employee is usually less interested in Information Security matters than in getting his or her work done as quickly as possible. Especially during times of stress, security measures are usually one of the first things to be ignored to speed up a process. When confronted with such measures, especially the trade-off between security vs. availability of services, employees often experience a feeling of hostility against these measures and those responsible for their implementation. Any attempt to implement Information Security policies under such adverse circumstances is sure to fail.

This poses one of the greatest challenges in the implementation of Information Security policies. In order for such an implementation to succeed, allies in other departments are needed to ensure people's cooperation to the extent required. This can only happen if everyone understands the reasons for the implementation of Information Security policies. In order to win them as allies, one must understand where they are coming from when it comes to Information Security. Simply being aware of the dangers that these policies and the measures that go along with them are trying to protect them from may not be enough. Ideally, they must be brought to a point of awareness where they willingly act as eyes and ears of the Information Security department throughout the entire company; indeed, this is the only way that such a department within a large company will be able to handle the enormous task that Information Security represents. This is especially difficult in the face of concerns about the possible invasion of privacy due to security measures.

Creating such awareness is key in the process of implementing Information Security policies. When everyone knows what is at stake and the consequences of failure in Information Security become clear, the efforts and members of the Information Security department are no longer seen as disablers, but as enablers for a more secure work environment for all employees. They become simply one more part of the company, doing its part for the success of the company rather than merely making other people's life harder than it already is.

The good implementation of Information Security policies normally requires a generous budget. In practice, the budget for Information Security is always short, as many managers still tend not to see Information Security as a key factor in a business' success. Since maintaining Information Security policies is an ongoing and evolving process, further budget is always required, but this subject is often viciously fought over during budget meetings. One challenge is therefore to convince management of why Information Security must be a top priority within the company and getting management's public support, top-down, for every

employee to see. One way to do so is through the help of allies and so-called ‘hidden opinion leaders’, supporting one’s position and arguments in this matter when they are presented to management. This thesis uses the term ‘hidden opinion leaders’ to denote people who have significant influence on the decisions made by management. Through extensive know-how and competence in their field, these employees have a level of expertise that has made them management’s choice when it comes to getting a reliable opinion on something that falls into their field of work and deciding whether further budget is to be granted. Winning them as allies and getting their support is therefore crucial to debates with management over budget issues.

As has already been suggested, Information Security is by definition an ongoing process. As such, it requires constant attention and maintenance and must always endeavor to stay ahead of the dangers that it tries to protect a company from. If this goal is to be achieved, Information Security processes must try to follow a proactive instead of a reactive approach. Since not every scenario can be anticipated, this is something that cannot be guaranteed, yet best efforts as well as proper training are required to raise and maintain the necessary level of awareness among all employees of a company.

Finally, regular audits and penetration tests should also be performed in order to evaluate the efficiency of current Information Security and its compliance with legislative and contractual commitments.

5. Recommended Approach

Approaching the challenges faced in the implementation of Information Security policies, one has to start by familiarizing oneself with the company requiring Information Security. This includes corporate design and structure, management style etc., and is usually done by first interviewing all departments even remotely related to Information Security, then management.

The reason for interviewing management is to determine its view on Information Security and the factors that management views as important. In order to gain management compliance for future projects, these factors need to be addressed first, even if they are not as important as others that may already have been identified (with the exception of critical findings of course). Once these are resolved and management is satisfied by this success, one can ensure its support for upcoming changes as well as for Information Security in general. Only then does the actual implementation process begin.

(1) The first phase is one of information gathering. In general, as much information as possible needs to be found to form an overview of where the company currently stands on the subject of Information Security. Besides conducting interviews, all documentation materials, policies, guidelines and information about currently applied Information Security tools and procedures need to be found and reviewed for their reusability. Additionally, people responsible for these materials need to be identified as they may become valuable allies. Of equal value is any information about unfinished or abandoned Information Security projects and the reasons for their abandonment. In many cases, such abandoned projects are founded on a perfectly adequate idea and were cancelled only for budgetary reasons. Knowing this and talking to the people responsible for these projects can make the process of Information Security policies implementation that much easier, as problems that these people have met in the past are recognized and can be avoided in the future. Old audit documentation can also

give valuable insight into what went wrong until now in terms of Information Security and what the consequences were. At the end of this phase, one should have an overview of the existing materials and documentation and know what can be of use. Everything else should simply be discarded.

(2) The next phase is the search for allies within other departments, especially User Management and User Support, Human Resources, Public Relations, Corporate Security, Legal and Documentation. These departments' areas of expertise are of great value during the process of implementing Information Security policies. Keeping a good relationship with them is therefore imperative. Beyond these departments and the fact that one goal of Information Security policies is to have each and every employee acting as the company's eyes and ears regarding Information Security, other important allies are the so-called 'hidden opinion leaders' and auditors. If treated as allies, auditors will likely respond as such and aid one in the common struggle of hardening a company's Information Security. By making them allies, one can place ideas directly in front of management by letting the auditors present them. An auditor's report goes directly to management; it states what has to be done to improve the company's current situation. If one's ideas find their way into these reports, they will more likely get approved by management, along with the necessary budget.

(3) After finding allies to support one's goal in implementing Information Security policies, it is time to identify the ways by which information spreads within the company, i.e. established communication channels, and who controls them, and make these people allies as well (if they are not already). These channels can then be used to spread Information Security content, raise knowledge and interest in Information Security and, along with combined training, raise the awareness of its audience.

(4) It is not enough for employees to simply know that there is someone within the company who is responsible for Information Security. This person/department has to be known or, even better, respected for his/its work and the ability to make a positive contribution to the company's operations by making them more secure. Essential in achieving this is the development of networking and leadership skills that support one's efforts to implement Information Security policies.

(5) A major factor in building and maintaining the necessary level of employee awareness is proper training. This requires state-of-the-art training methods and tools as well as frequent repetition and attendance control. A specialized training is presented to new employees, starting with orientation day. If the necessary resources for this are not to be found within a company, this task can be outsourced to companies specialized in this area.
(6) Every effort undertaken for the implementation of Information Security policies requires budget. Getting the budget can be seen as a selling process with the Information Security ideas as goods and management as the prospective buyers. The best way to closing such a deal is through getting the necessary support from allies and 'hidden opinion leaders' whose influence can make a substantial difference in getting a much needed budget approved. Beyond that support, the ideas that are to be sold must be presented in a way that leaves no doubt about why an approval of the necessary budget is needed. The key to this are simple messages with an easily recognizable, bottom-line conclusion. This should be repeated throughout the presentation as well as in the summary documents sent out to management and involved departments after the presentation.

(7) At some point, management will want to evaluate the efforts in implementing Information Security policies it has funded. This often presents a dilemma, as the success of all security

measures is reflected in by the absence of security incidents. In other words – if nothing happened, this most likely means that the Information Security policies were successfully implemented and are working as intended. By itself, however, that will not get the next budget approved; what is needed instead are data, hard facts, numbers and statistics that can be reviewed by management and prove the success of the Information Security policies implementation.

6. Conclusion and outlook

Implementing Information Security policies is not a simple task. During the process of implementation, one might even reach the surprising conclusion that the greatest challenges faced in Information Security have nothing to do with ill-meaning persons or criminals intending to steal a company's valuable information security assets, but with the very people whose information assets one is trying to protect through Information Security policies and measures. An adversarial approach, however, in which one tries to force Information Security onto employees, is sure to fail. Indeed, success in the implementation of Information Security policies and efficiency in their application can only come through working together, with a company's employees and within a company's culture, not against them.

This realization has its value, yet good will alone does not suffice, as the relationship between Information Security professionals and other employees is often tense. This stems from an unfortunate, but inevitable downside of Information Security: As a result of optimizing work processes in terms of Information Security, these processes become more complex than they were before. A natural and, up to a point, even understandable reaction to this fact is therefore that employees resist Information Security measures. Such resistance needs to be overcome, as the most significant asset in one's arsenal for protecting a company's information assets is the awareness of those very employees – awareness of the value of information, the threats that they face while handling information assets, and the need for Information Security, with all the implications this has for a company's business.

As if this were not enough of a challenge already, working in a field where success is defined through the absence of incidents, the Information Security department constantly needs to justify its existence in the eyes of management. Getting the budget to build and maintain an ongoing Information Security program, devising policies and conducting their implementation is another substantial challenge faced by the Information Security department of any given company.

Both of these challenges can only be overcome by accepting that the implementation of Information Security policies is, in fact, a sales matter in which one needs to sell Information Security principles and measures to the employees of a company (so that they will be followed by them) and its management (so that the necessary budget will be granted to implement these measures). This requires not only in-depth knowledge about one's company, its employees, management and culture, but persuasive strategies that can only work with the help of allies throughout the company. Such allies are thus necessary for their support of the principles of Information Security as a continuous process and to establish the necessity for Information Security policies within a company.

While technology-based challenges for Information Security become more advanced as time passes, so do the technical means to counter these challenges. The implementation of Information Security policies, however, remains a challenge that is and will remain primarily

a people matter that requires corresponding approaches to solve it. While this thesis' goal was to present such an approach, it must be acknowledged that such approaches may be as diverse as people's attitudes toward Information Security, making the further study of viable approaches for the implementation of Information Security policies a subject of continuing interest.

universität wien

MASTERARBEIT
Zusammenfassung

Titel

Challenges in Implementing Information Security policies

Verfasser

Andreas Reichard

angestrebter akademischer Grad

Diplomingenieur

Wien, 2010

Studienkennzahl lt. Studienblatt:	A 066 926
Studienrichtung lt. Studienblatt:	Wirtschaftsinformatik
Betreuer:	Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

1. Einführung

Grundsätzlich kann jeder Form von Information ein bestimmter Wert zugeordnet werden. Die genaue Höhe dieses Wertes hängt von Faktoren wie dem Inhalt der Information, dem Grad der Geheimhaltung der sie unterliegt, ihrem Besitzer etc. ab. In manchen Fällen, v.a. im Geschäftsbereich, kann dieser Wert monetär ausgedrückt werden; in anderen Fällen ist dies nicht möglich. Unklarheit über die möglichen Konsequenzen für den Fall, dass solche Information in die falschen Hände gerät, hat zur Entwicklung von Maßnahmen geführt, die dies verhindern sollen. Der entsprechende Umgang mit Information – nicht ausschließlich solcher, die einer besonderen Geheimhaltung unterliegt, sondern generell – auf eine Weise, welche Business Prozesse nicht unnötig behindert, gleichzeitig aber die Information selbst vor unerwünschtem Zugriff schützt, fällt in den Bereich der Informationssicherheit (engl. ‚Information Security').

Die Erkenntnis über die Gefahr einer unerwünschten Verbreitung von Informationen hat dazu geführt, dass Unternehmen großen Aufwand an Zeit und Geld in die Erstellung eines Informationssicherheitsprogramms investieren. Der hierfür nötige Aufwand allein garantiert allerdings nicht die Effizienz eines solchen Programms in seiner Anwendung, d.h. er bedingt nicht, dass die betroffenen Personen auch damit einhergehen und, wenn ja, bis zu welchem Grad sie dies tun. Eine Investition in das Design eines Informationssicherheitsprogramms ohne ausreichende Kenntnis der Auswirkungen, die es auf Personen haben wird, wird mit hoher Wahrscheinlichkeit zu einer Diskrepanz zwischen Konzeption und Anwendung eines solchen Programms führen. Im schlimmsten Fall kann dies sogar das gesamte Programm untergraben, nämlich dann, wenn die betroffenen Personen den allgemeinen Nutzen des Programms für sie und das Unternehmen nicht erkennen können. In so einem Fall werden sie der Effizienz in der Bearbeitung ihrer alltäglichen Verantwortlichkeiten die höchste Priorität beimessen, die Informationssicherheit aber vernachlässigen. Dass damit die Verletzung einer Zahl von Informationssicherheitsmaßnahmen einhergeht, die eigentlich dem Schutz wertvoller Informationen dienen sollten, ist mit hoher Wahrscheinlichkeit anzunehmen.

Die vorliegende Arbeit unterscheidet zwischen dem Design und der Umsetzung eines Informationssicherheitsprogramms. In diesem grundlegenden Unterschied liegt die Ursache für die mögliche Kluft zwischen Konzeption und Anwendung eines solchen Programms. Die Frage, die diese Arbeit daher zu beantworten sucht, ist folgende: Wie kann diese Kluft zwischen Konzept und Anwendung reduziert werden oder aber, genauer gesagt, Informationssicherheit den betroffenen Personen, Mitarbeitern wie Managern, so kommuniziert werden, dass diese ihren Wert für sie persönlich wie auch für das Unternehmen erkennen? Nur durch ein solches Verständnis, d.h. entsprechendes Bewusstsein, kann das Befolgen eines Informationssicherheitsprogramms erreicht werden, und damit schließlich auch seine Umsetzung wie vom Design her vorgesehen.

Obwohl die erfolgreiche Umsetzung eines Informationssicherheitsprogramms mit seiner Konzeption und Erstellung zusammenhängt, liegt der Fokus dieser Arbeit nicht auf dem Design eines solchen Programms. Zwar ergeben sich aufgrund des erwähnten Zusammenhangs insofern gewisse Berührungspunkte, als einige wichtige Aspekte des Designs eines Informationssicherheitsprogramms aufgezeigt werden, das Hauptaugenmerk dieser Arbeit liegt jedoch auf der Überwindung möglicher Hindernisse, die sich während der Implementierung von Richtlinien für Informationssicherheit ergeben und die Effizienz eines entsprechenden Programms schmälern können. Dadurch kann die Akzeptanz eines Informationssicherheitsprogramms maximiert werden, da es von den betroffenen Personen als

Maßnahme gesehen wird, die Information als ein gemeinsames Gut vor unerwünschtem Zugriff schützt.

2. Der Wert von Information

Jedes Unternehmen besitzt Güter denen ein bestimmter Wert zugeordnet werden kann. Der Verlust dieser Güter kommt also einem Verlust für das sie besitzende Unternehmen gleich. Dieser Verlust ist umso größer, je stärker diese Güter mit dem Unternehmen auf spezielle Art verbunden sind. In dieser Hinsicht sind auch die Informationen eines Unternehmens auf viele unterschiedliche Arten speziell mit diesem verbunden. Unterschiedliche Arten von Information können unterschiedliche Werte für verschiedene Personen haben. Fest steht, dass es für jede Art von Information jemanden gibt, für den diese einen bestimmten Wert hat. Dies trifft auch für scheinbar unverfängliche Information zu. In weiterer Folge sollte daher jede Art von Information eines Unternehmens gegen den unerwünschten Zugriff und einen möglichen Missbrauch geschützt werden.

Scheinbar unverfängliche Information in den Händen einer Person, welche weiß, wie sie gewinnbringend anzuwenden ist, kann zu großem Schaden für ein Unternehmen führen. Sogenannte ‚Social Engineers' haben sich mittels linguistischer und psychologischer Methoden darauf spezialisiert, genau diese Art von Information nichts ahnenden Mitarbeitern zu entlocken. Diese Information kann später zum Schaden eines Unternehmens verwendet werden, z.B. bei Wirtschaftsspionage, Erpressung, aber auch privat motivierter Bereicherung wie z.B. Identitätsdiebstahl.

Heutzutage stellt Identitätsdiebstahl eine der häufigsten Verwendungen für gestohlene Information dar. Durch die Verbreitung von Online Communities, E-Commerce usw. haben sich viele Personen eine Vielzahl an virtuellen Identitäten geschaffen. Der Grund für die Existenz solcher virtuellen Identitäten, jedenfalls aus der Perspektive jener Institution, welche solche verleiht (d.h. ein Unternehmen das E-Commerce betreibt), ist die Etablierung einer Repräsentanz des Besitzers einer virtuellen Identität über welche kommuniziert und Handel betrieben werden kann. Dies bedeutet weiters, dass aus der Sicht einer solchen Institution eine solche virtuelle Identität äquivalent ist zu dem Besitzer dieser Identität. Jede Form von Handlung, die über diese virtuelle Identität getätigt wird, wird damit dieser Person zugeordnet und davon ausgegangen, dass diese sie wissentlich und zustimmend getätigt hat.

Die Verbreitung von E-Commerce über das Internet hat gezeigt, dass dieses Konzept globale Märkte eröffnet und es Unternehmen wie Kunden ermöglicht hat, miteinander in Kontakt zu treten und Geschäfte abzuwickeln. Unglücklicherweise hat dieses Konzept jedoch auch einige Probleme aufgeworfen. Eines der gravierendsten davon ist die illegale Verwendung virtueller Identitäten durch Personen welche nicht die ursprünglichen Besitzer dieser Identität sind. Diesen Fall bezeichnet man als Identitätsdiebstahl. Dies stellt insofern ein Problem dar, als dass aus der Sicht des Unternehmens, welches virtuelle Identitäten aushändigt, jede über die Verwendung einer solchen Identität getätigte Handlung automatisch jener Person zugeordnet wird, welche diese Identität ursprünglich registriert hat. Der Zugriff auf eine solche virtuelle Identität auf illegalem Weg und deren Benutzung für kriminelle Zwecke ist damit eine Möglichkeit, jemand anderen (den ursprünglichen Besitzer der virtuellen Identität) für Handlungen verantwortlich zu machen, die dieser tatsächlich nicht begangen hat, während man wahrscheinlich selbst davon profitiert.

Der Diebstahl virtueller Identitäten ist eine der jüngsten Erscheinungen, die durch die Ausbreitung des Internets aufgetreten sind. Das grundliegende Problem ist jedoch nicht Internet-spezifisch. Wo auch immer Personen involviert sind, gibt es viele Situationen in denen sie sich gegenüber anderen mit Hilfe einer virtuellen Identität ausweisen, um Zugang zu geheimen Daten zu erlangen (z.B. Konto-Zugangsdaten, Pin Codes etc.). In jeder dieser Situationen besteht die Möglichkeit, sich über den Diebstahl einer solchen virtuellen Identität (z.B. durch Erlangung eines dafür notwendigen Zugangscodes) Zugang zu diesen Daten zu verschaffen, während man sich als der eigentliche Besitzer dieser Identität ausgibt. Solche Fälle zählen ebenfalls zu Identitätsdiebstahl, selbst wenn sie nicht im Internet auftreten, sondern in der sogenannten ‚realen Welt'.

3. Richtlinien für Informationssicherheit

Der Wert, welcher einer bestimmten Information zugewiesen wird, kann das Ergebnis der subjektiven Entscheidung einer bestimmten Person sein. Basierend auf dieser Entscheidung wird dieser Information dann ein bestimmter Grad an Vertraulichkeit zugewiesen, möglicherweise wird die Information auch an andere Personen weitergegeben. Aufgrund der Subjektivität einer solchen Entscheidung variiert auch der Grad an Vertraulichkeit, mit dem eine Information behandelt wird, zwischen unterschiedlichen Personen. Dieser Zustand ist im Sinne einer ernstzunehmenden Informationssicherheit nicht akzeptabel.

Dieser grundlegende Befund erfordert daher eine Sammlung an Dokumenten, Regeln und Richtlinien, welche den Grad an Vertraulichkeit sowie die Personen, die Zugriff auf Informationen haben, festlegen. Diese müssen so verfasst sein, dass keinerlei Zweifel offen bleiben über die Art und Weise, wie Informationen zu handhaben sind. Eine solche Sammlung an Dokumenten bezeichnet man als ‚Richtlinien für Informationssicherheit'. Diese sind keineswegs statischer Natur, sondern müssen regelmäßig überprüft und ggf. angepasst werden, sollte es sich als notwendig erweisen (z.B. aufgrund einer technischen Änderung oder einer Entscheidung des Managements).

Richtlinien für Informationssicherheit bestehen zumindest aus den folgenden Teilen (wobei bei Bedarf weitere hinzugefügt werden können):

- Policy statement
- Standards
- Procedures
- Principles
- Guidelines
- Classifications (Level an Vertraulichkeit, Zugangsbeschränkungen, Zwischenfall Klassifizierungen)
- Definition von Termini

Die Verantwortlichkeiten bzgl. der Richtlinien für Informationssicherheit müssen in einem Unternehmen klar definiert sein. Dies beinhaltet deren Etablierung, Management, Wartung, Überprüfung und Überarbeitung, Durchsetzung und Exekutierung im Falle von Verstößen und gerichtlichem Vorgehen. Die entsprechende Dokumentation muss auch den Lebenszyklus der Richtlinien festlegen, d.h. wann diese überprüft, angepasst, verworfen oder durch eine neue Version ersetzt werden sollen.

Der Gültigkeitsbereich von Richtlinien für Informationssicherheit hängt einerseits von der Größe des zu schützenden Unternehmens ab, andererseits von seinen Geschäftsverbindungen ins In- und Ausland. Richtlinien für Informationssicherheit, welche sich ausschließlich mit einem einzigen Unternehmen befassen, sind unzureichend, wenn dieses Unternehmen Partner hat, welche nicht dieselben Ansichten bzgl. Informationssicherheit teilen. Nachdem diesen Partnern im Zuge der Partnerschaft oft Zugriff auf vertrauliche Daten gewährt werden muss, kann es dabei zu Verstößen gegen die Richtlinien für Informationssicherheit kommen. Dies hat zur Folge, dass diese Richtlinien im Sinne der Informationssicherheit praktisch wirkungslos sind, nachdem die kritische Frage ob ihrer möglichen Verletzung nicht durch die entsprechenden Richtlinien behandelt wird, sondern lediglich an das Partnerunternehmen weitergegeben wurde. Dieses stellt somit ein Informationssicherheitsrisiko für das eigene Unternehmen dar. Es ist daher notwendig, Richtlinien für den korrekten Umgang mit Information innerhalb von Geschäftspartnerschaften mit den eigenen Richtlinien für Informationssicherheit abzugleichen. Hier ist insbesondere auf mitunter unterschiedliche Gesetzeslagen bei internationalen Partnerschaften zu achten.

Im Fall eines Informationssicherheitszwischenfalls hat eine Reihe von Kettenreaktionen statt zu finden. Diese beinhalten u.a. die Klassifizierung des Zwischenfalls, eine entsprechende Reaktion und Reporting. Die Reaktion hängt von der Klassifizierung ab, welche der Zwischenfall erhalten hat. Diese Klassifizierungen müssen daher, ebenso wie die zusammenhängenden Reaktionen, bereits vorab als fixer Bestandteil der Richtlinien für Informationssicherheit definiert werden.

Ein wichtiger Teil des Lebenszyklus von Richtlinien für Informationssicherheit ist ihre regelmäßige Überprüfung und ggf. Überarbeitung, sollte dies erforderlich sein. Dies impliziert auch die Verantwortung, ständig auf dem neuesten Stand zu sein bzgl. neuer Gefahren für die Informationssicherheit, aufgetretener Informationssicherheitszwischenfälle sowie neuer Produkte welche helfen können, diese Gefahren einzudämmen. Diese Verantwortung muss ebenfalls klar definiert werden. Ein guter Überblick darüber sowie über die Ressourcen des eigenen Unternehmens ist unerlässlich, um eine realistische Prognose darüber erstellen zu können, welche Gefahren dem Unternehmen drohen könnten und wie ihnen am besten zu begegnen wäre.

4. Hindernisse in der Implementierung von Richtlinien für Informationssicherheit

Die Implementierung von Richtlinien für Informationssicherheit beinhaltet zahlreiche notwendige Maßnahmen, erfordert aber auch die Akzeptanz jener Personen, deren Arbeitsalltag durch diese Richtlinien erschwert wird. Der durchschnittliche Angestellte ist normalerweise eher daran interessiert, seine Arbeit so schnell wie möglich abzuwickeln, als an Informationssicherheit. Besonders unter Stress sind Sicherheitsmaßnahmen oft eines der ersten Dinge welche umgangen werden um einen Arbeitsprozess zu beschleunigen. Werden Angestellte mit diesen Maßnahmen konfrontiert, insbesondere im Fall eines Konflikts zwischen Sicherheit und Verfügbarkeit (engl. ‚Security vs. Availability trade-off'), so ist ihre Reaktion oft ablehnend ggn. den Maßnahmen sowie den Verantwortlichen, die für ihre Umsetzung Sorge tragen. Ein Versuch, unter solchen Umständen die Umsetzung solcher Maßnahmen zu erreichen, ist häufig zum Scheitern verurteilt.

Dieser Umstand stellt eine der größten Herausforderungen in der Etablierung von Richtlinien für Informationssicherheit dar. Um eine Implementierung dieser Richtlinien zum Erfolg zu

führen, bedarf es der Unterstützung durch Verbündete in anderen Abteilungen, um die Kooperation der Angestellten zu gewinnen, ohne die es keine Informationssicherheit geben kann. Dies kann nur dann passieren, wenn alle Betroffenen die Gründe für eine solche Implementierung kennen und verstanden haben. Um diese Personen als Verbündete zu gewinnen muss zunächst verstanden werden, wie sie zu ihren ursprünglichen Ansichten bzgl. Informationssicherheit kamen. Nur das Wissen allein über die Existenz von Gefahren, welche durch die Richtlinien für Informationssicherheit und damit verbundene Maßnahmen abgewendet werden sollen, ist nicht ausreichend. Idealerweise sollen die betroffenen Personen ein Bewusstsein für diese Dinge erlangen, so dass sie von sich aus aufmerksam für mögliche Gefahren bleiben und somit die Informationssicherheitsabteilung in ihrer Arbeit unterstützen. Dies ist tatsächlich der einzige Weg, wie eine solche Abteilung innerhalb eines großen Unternehmens die schier ausufernde Aufgabe, welche die Aufrechterhaltung von Informationssicherheit ausmacht, bewältigen kann. Erschwerend wirken sich dabei auch mögliche Bedenken ob einer möglichen Verletzung der Privatsphären der Mitarbeiter durch Sicherheitsmaßnahmen aus, welche im Zuge einer Implementierung von Richtlinien für Informationssicherheit seitens der Mitarbeiter aufkommen können.

Auf dem Entstehen eines solchen Bewusstseins liegt ein Hauptaugenmerk im Prozess der Implementierung von Richtlinien für Informationssicherheit. Wenn jeder weiß, was auf dem Spiel steht, und die möglichen Konsequenzen eines Informationssicherheitszwischenfalls realisiert, werden die Bemühungen der Informationssicherheitsabteilung nicht mehr als behindernd, sondern als fördernd wahrgenommen. Die Abteilung wird dann zu einer von vielen Abteilungen, welche ihren Teil zum gemeinsamen Erfolg des Unternehmens beiträgt, anstatt nur den Arbeitsalltag ihrer Kollegen zu erschweren.

Die gute Implementierung von Richtlinien für Informationssicherheit erfordert normalerweise ein entsprechendes Budget. In der Praxis ist das Budget für Informationssicherheit jedoch stets knapp, da viele Manager Informationssicherheit immer noch nicht als eine Priorität für den Erfolg eines Unternehmens ansehen. Nachdem die Aufrechterhaltung von Richtlinien für Informationssicherheit ein steter Prozess ist, ist ebenso ein stetes Budget dafür erforderlich. Dies ist jedoch ein Umstand, der in Budgetmeetings oft heftig diskutiert wird. Eine Herausforderung ist es daher, das Management davon zu überzeugen, warum Informationssicherheit eine Priorität für das Unternehmen sein muss, und dafür seine Unterstützung einzuholen, die top-down im gesamten Unternehmen für jeden Angestellten sichtbar sein muss.

Dies kann durch die Unterstützung sgn. ‚Hidden opinion leaders' im Unternehmen erfolgen, welche die eigene Position und Argumente unterstreichen, wenn diese zur Erlangung von Budget für weitere Informationssicherheitsmaßnahmen an das Management herangetragen werden. Diese Arbeit benutzt den Terminus ‚Hidden opinion leaders' für Personen welche einen signifikanten Einfluss auf die Entscheidungen des Managements haben. Durch starkes Know-How und Kompetenz in ihrem Arbeitsumfeld haben diese Personen einen Grad an Expertise erlangt, der sie bei Budgetfragen zu einer verlässlichen Anlaufstelle für das Management macht, wenn es um die Beurteilung einer Angelegenheit geht, die in deren Kompetenz fällt. Ihre Unterstützung ist daher von höchster Wichtigkeit in solchen Budgetmeetings.

Wie bereits festgehalten wurde ist Informationssicherheit ein steter Prozess. Als solcher erfordert er ständige Aufmerksamkeit und Wartung sowie das Bestreben, etwaigen Gefahren für ein Unternehmen bereits einen Schritt voraus zu sein, um dieses davor schützen zu können. Wenn dieses Ziel erreicht werden soll, muss Informationssicherheit anstatt eines

reaktiven einen aktiven Weg verfolgen. Zwar mag nicht jedes denkbare Szenario, in dem sich ein Unternehmen bzgl. Informationssicherheit finden könnte, vorausgesagt werden können, doch sollte zumindest das Möglichste in diese Richtung versucht werden, einschließlich entsprechendem Training zur Erreichung und Erhalt des dafür erforderlichen Bewusstseins für Informationssicherheit bei den betroffenen Personen.

Regelmäßige Audits und sogenannte ‚Penetration Tests' sollten ebenfalls stattfinden, um die Effizienz der aktuellen Informationssicherheit und ihre Übereinstimmung mit der aktuellen Gesetzeslage und etwaigen vertraglichen Verpflichtungen zu überprüfen.

5. Empfohlene Vorgehensweise

Bei der Auseinandersetzung mit möglichen Hindernissen bei der Implementierung von Richtlinien für Informationssicherheit sollte man zuerst damit beginnen, sich mit dem Unternehmen, welches diese Richtlinien benötigt, vertraut zu machen. Das beinhaltet Kenntnis von Corporate Design, Struktur des Unternehmens, Management Stil etc. Diese Informationen werden üblicherweise über Interviews mit allen betroffenen Abteilungen, welche auch nur im Entferntesten mit Informationssicherheit zusammenhängen, bezogen und danach in Gesprächen mit dem Management selbst ergänzt.

Der Zweck der Interviews mit dem Management liegt darin, herauszufinden, was aus der Sicht des Managements Informationssicherheit bedeutet sowie welche Prioritäten diesbzgl. existieren. Um den Zuspruch oder zumindest das Wohlwollen des Managements für künftige Projekte zu erlangen, sollte man sich den Faktoren, die während dieser Interviews identifiziert werden, zuerst widmen, selbst wenn ihre tatsächliche Bedeutung hinter der anderer Faktoren liegt, die man bereits identifiziert hat. Dies soll dazu dienen, dem Management möglichst schnell Erfolge präsentieren zu können, was in weiterer Folge die Chance auf Unterstützung für weitere Maßnahmen zur Steigerung der Informationssicherheit erhöht. Daher sollte erst wenn diese Faktoren abgehandelt wurden, d.h. günstige Ausgangsbedingungen geschaffen wurden, der eigentliche Implementierungsprozess beginnen.

(1) Die erste Phase dieses Prozesses befasst sich mit Informationseinholung. Generell sollte so viel Information wie möglich über den aktuellen Stand des Unternehmens bzgl. Informationssicherheit eingeholt werden. Neben der bereits angesprochenen Durchführung von Interviews müssen alle Dokumentationsmateralien, Richtlinien, Guidelines und jede sonstige Information über aktuell verwendete Informationssicherheitswerkzeuge und Prozeduren identifiziert und bzgl. ihrer Wiederverwendbarkeit beurteilt werden. Personen, die dafür verantwortlich sind oder waren, sind ebenfalls ausfindig zu machen, da sie wertvolle Verbündete darstellen können. Ebenso wichtig sind Informationen über unfertige oder abgebrochene Informationssicherheitsprojekte, sowie die Ursache dafür, dass diese nicht fertig gestellt wurden. In vielen Fällen ist die einem solchen Projekt zugrundeliegende Idee verfolgenswert, das Projekt wurde nur aus budgetären Gründen nicht durchgeführt und kann möglicherweise wieder aufgenommen werden. Die für diese Projekte verantwortlichen Personen verfügen möglicherweise über Wissen von den Problemen, die sich damit ergaben, so dass man dieselben Probleme bei ähnlichen, künftigen Projekten nicht gänzlich unvorbereitet antrifft. Dies kann den Prozess einer Implementierung von Richtlinien für Informationssicherheit erheblich beschleunigen. Alte Audit Dokumentationsmaterialien geben außerdem Auskunft darüber, was bis zum gegebenen Zeitpunkt bzgl. Informationssicherheit im Unternehmen falsch gemacht wurde und welche Konsequenzen aus diesen Erkenntnissen gezogen wurden. Am Ende dieser Phase sollte man einen guten Überblick darüber haben,

welche Materialien und Dokumentationen existieren und was davon weiterhin verwendet werden kann. Das übrige Material kann dann getrost verworfen werden.

(2) Die nächste Phase besteht aus der Suche nach Verbündeten in anderen Abteilungen, besonders User Management und User Support, Human Resources, Public Relations, Corporate Security, die Rechtsabteilung sowie die Dokumentationsabteilung. Die Expertise dieser Abteilungen ist von großem Wert während des Implementierungsprozesses. Es ist daher wichtig, ein gutes Verhältnis zu ihnen zu bewahren. Darüber sowie über das Ziel hinaus, das Bewusstsein jedes Angestellten eines Unternehmens für Informationssicherheit soweit zu schärfen, so dass diese stets aufmerksam bzgl. möglicher Gefahren bleiben, sind weitere wichtige Verbündete die sogenannten ‚Hidden opinion leaders' in einem Unternehmen sowie Auditoren. Letztere werden, wenn man sie wie Verbündete behandelt, sich auch wie solche verhalten und einen in der gemeinsamen Aufgabe der Erhöhung der Informationssicherheit des Unternehmens unterstützen. Dies kann etwa dadurch geschehen, dass eigene Ideen den Auditoren so präsentiert werden, dass diese die Vorschläge dann in die Audit Reports aufnehmen. Diese Reports, welche die Empfehlungen der Auditoren zur Verbesserung der Informationssicherheit im Unternehmen enthalten, gehen meist direkt an das Management und werden daher mit entsprechend hoher Priorität von diesem behandelt. Sollten sich die eigenen Ideen zur Verbesserung der Informationssicherheit in diesen Reports wiederfinden, so wirkt sich das bei der Frage nach der Zusage für ein entsprechendes Projekt sowie dem entsprechenden Budget für die Umsetzung dieser Ideen seitens des Managements entsprechend positiv aus.

(3) Nach der Suche nach Verbündeten zur Implementierung von Richtlinien für Informationssicherheit ist es an der Zeit, die Kanäle, über die Informationen innerhalb des Unternehmens publiziert werden, ausfindig zu machen, sowie jene Personen/Abteilungen, welche diese kontrollieren. Sofern dies noch nicht geschehen ist, sollten diese ebenfalls zu Verbündeten gemacht werden. Die Informationskanäle können dann dazu benutzt werden, Informationssicherheits-Content zu publizieren, um Wissen sowie das Interesse für Informationssicherheit zu erhöhen sowie, in Kombination mit entsprechendem Training, das Bewusstsein für Informationssicherheit zu steigern.

(4) Es reicht nicht aus, dass Mitarbeiter eines Unternehmens wissen, dass es jemanden gibt, der für Informationssicherheit im Unternehmen verantwortlich ist. Diese Person oder Abteilung muss sichtbar und bekannt sein, oder besser noch, für ihre Arbeit respektiert werden, welche als ein positiver Beitrag zum gemeinsamen Arbeitsziel gesehen werden soll. Um dies zu bewerkstelligen sind Netzwerk- und Führungsqualitäten gefragt, welche die Bemühungen zur Implementierung von Richtlinien für Informationssicherheit unterstützen.

(5) Ein entscheidender Faktor in der Herstellung und Erhaltung des notwendigen Grads an Bewusstsein für Informationssicherheit unter Mitarbeitern ist entsprechendes Training. Dies bedarf aktuellster Trainingsmethoden und Werkzeuge sowie regelmäßiger Wiederholung der Trainings und einer Teilnahmekontrolle. Während der Einführungstage erfahren neue Mitarbeiter ein spezielles Training. Sind die notwendigen Ressourcen für das erforderliche Training nicht im Unternehmen verfügbar, so kann diese Aufgabe an andere Unternehmen ausgelagert werden.

(6) Jede Bemühung im Rahmen der Implementierung von Richtlinien für Informationssicherheit erfordert in der Regel ein Budget. Die Anstrengungen, dieses bewilligt zu bekommen, können mit einem Verkaufsgespräch verglichen werden, wobei die Ideen zur Erhöhung der Informationssicherheit als Gut und das Management als potentieller Käufer

betrachtet werden können. Die höchsten Erfolgschancen in so einem Gespräch erzielt man über die Unterstützung von Verbündeten und ‚Hidden opinion leaders', deren Einfluss in so einer Situation entscheidend darüber sein kann, ob ein dringend benötigtes Budget bewilligt wird oder nicht. Abseits dieser Unterstützung bedarf es aber auch einer Präsentation der zu ‚verkaufenden' Ideen, welche keinen Zweifel darüber offen lässt, warum das dafür erforderliche Budget unbedingt bewilligt werden muss. Entscheidend dabei sind einfache, kurze Nachrichten und eine simple, einprägsam formulierte Schlussfolgerung, zu welcher im Zuge der Präsentation immer wieder zurückgekehrt wird. Gut aufbereitete Zusammenfassungsdokumente, welche an das Management und alle betroffenen Abteilungen versandt werden, runden die Präsentation ab.

(7) Zu einem bestimmten Zeitpunkt wird das Management die Maßnahmen zur Implementierung von Richtlinien für Informationssicherheit, für die ein Budget bewilligt worden ist, evaluieren wollen. Dies stellt insofern ein Dilemma dar, als dass Erfolge in Sicherheitsfragen hauptsächlich durch das Ausbleiben eventueller Zwischenfälle angezeigt werden. Dies heißt in anderen Worten – wenn nichts passiert ist, lässt das darauf schließen, dass die Richtlinien für Informationssicherheit korrekt implementiert wurden und wirksam sind. Das allein wird allerdings kaum helfen, das Budget für dringend anstehende Maßnahmen zu sichern, es müssen daher ‚harte' Fakten, Zahlen, Statistiken etc. identifiziert werden, die dem Management vorgelegt werden können, um zu belegen, dass das bislang in die Informationssicherheit investierte Budget sinnvoll verwendet wurde und dies daher bei weiteren Investitionen ebenso der Fall sein wird.

6. Resümee und Ausblick

Die Implementierung von Richtlinien für Informationssicherheit ist keine simple Angelegenheit. Während des Implementierungsprozesses mag man sogar zu dem überraschenden Schluss gelangen, dass das größte Hindernis, welchem man in der Informationssicherheit begegnet, weniger mit der Bedrohung von Informationsgut eines Unternehmens durch Kriminelle oder Datendiebe zu tun hat, sondern mit eben jenen Personen, deren Gut durch die Richtlinien für Informationssicherheit und entsprechende Maßnahmen geschützt werden soll. Ein konfrontativer Zugang zu dieser Problematik, in dem man versucht, Mitarbeitern Informationssicherheit aufzuzwingen, wird jedoch fehlschlagen. Erfolg kann sich hier nur über eine kooperative Zusammenarbeit einstellen, *mit* den Mitarbeitern eines Unternehmens und innerhalb der Unternehmenskultur, nicht gegen sie.

Diese Erkenntnis hat ihren Wert, guter Wille allein ist jedoch nicht ausreichend, da die Beziehung zwischen der Informationssicherheitsabteilung und anderen Mitarbeitern eines Unternehmens oftmals angespannt ist. Dies resultiert aus einer unglücklichen, jedoch unvermeidlichen Nebenerscheinung der Informationssicherheit: Um Arbeitsprozesse im Sinne von Informationssicherheit zu optimieren, werden diese Prozesse zumeist komplexer als sie es zuvor waren. Es ist daher eine natürliche und bis zu einem gewissen Grad auch verständliche Reaktion, wenn Mitarbeiter gegen solche Maßnahmen im Zuge der Erhöhung der Informationssicherheit Widerstand hegen. Dieser Widerstand muss jedoch überkommen werden, da das Bewusstsein der Mitarbeiter bzgl. der Notwendigkeit für Informationssicherheit die wohl wichtigste Waffe im eigenen Arsenal gegen mögliche Bedrohungen darstellt, denen die Mitarbeiter in ihrem Arbeitsalltag und der Handhabung wertvoller Informationen begegnen.

Als wäre dies noch nicht Herausforderung genug, sieht sich die Informationssicherheitsabteilung dem ständigen Dilemma gegenüber, seine eigene Existenz bzw. die Durchführung seiner Maßnahmen und Projekte ggn. dem Management zu argumentieren, um das notwendige Budget zur Erstellung und Erhaltung des Informationssicherheitsprogramms, der Erstellung von Richtlinien und der Planung und Durchführung ihrer Implementierung bewilligt zu bekommen. Dies ist eine Herausforderung welche jede Informationssicherheitsabteilung in jedem Unternehmen bewältigen muss.

Beide Herausforderungen können nur bewältigt werden, wenn akzeptiert wird, dass die Implementierung von Richtlinien für Informationssicherheit tatsächlich nichts anderes ist als ein Verkaufsgeschäft, in dem Informationssicherheitsmaßnahmen den Mitarbeitern eines Unternehmens (auf dass diese sie befolgen mögen) sowie dem Management (auf dass dieses das nötige Budget dafür bewilligt) verkauft werden. Dies erfordert nicht nur tiefgründiges Wissen über das entsprechende Unternehmen, seine Mitarbeiter, das Management und die Unternehmenskultur, sondern auch ausgefeilte Überzeugungsstrategien welche nur mit Hilfe eines Netzwerks an Verbündeten zum Erfolg führen können. Die Unterstützung solcher Verbündeter ist notwendig, um Informationssicherheit als steten Prozess und das Bewusstsein ob seiner Notwendigkeit im Unternehmen aufrecht zu erhalten.

Während technologiebasierende Herausforderungen für die Informationssicherheit immer ausgereifter werden, gilt dies auch für entsprechende technische Gegenmaßnahmen. Die Implementierung von Richtlinien für Informationssicherheit ist jedoch eine Angelegenheit, die sich primär mit Menschen befasst und daher einen angemessenen Zugang erfordert. Diese Arbeit hat es sich zum Ziel gesetzt, Möglichkeiten für so einen Zugang herauszuarbeiten. Es muss jedoch festgehalten werden, dass ein solcher Zugang so unterschiedlich sein kann, wie die individuellen Einstellungen von Personen gegenüber der Informationssicherheit. Dadurch bleibt das weitere Studium der Durchführbarkeit von Möglichkeiten zur Implementierung von Richtlinien für Informationssicherheit auch in Zukunft eine herausfordernde Angelegenheit.

Curriculum Vitae

mit Schwerpunkt auf den wissenschaftlichen Werdegang

Andreas Reichard

Persönliche Daten:

Geburtsdatum: 17.02.1981 in Wien
Staatsbürgerschaft: Österreich
E-Mail: andreas.reichard@gmx.net

Akademische Laufbahn:

2006-2010 **Informatikmanagement** Magisterstudium an Universität Wien und Technischer Universität Wien
- Kernfachgebiet: **E-Business u. E-Government, Netzwerke**

2005-2006 **Erasmus** an der Universidad de Deusto, Bilbao
- Arbeit an Wirtschaftsinformatik Masterarbeit unter Prof. Anselmo del Moral Bueno
- Absolvierung mehrerer Lehrveranstaltungen im Bereich IT- und Information Security
- Vortrag über Social Engineering bei Security Konferenz „Kaslab Jornadas 2006" in Madrid

2001-2010 **Wirtschaftsinformatik** Bakkalaureats- und Masterstudium an Universität Wien und Technischer Universität Wien
- Kernfachgebiet Bakkalaureat: **E-Commerce**
- Kernfachgebiet Master: **Information Security, IT Security**
- Bakkalaureatsarbeit zum Thema „Social Engineering - Deceiving the Weakest Link in a Security Chain" unter Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr
- Masterarbeit zum Thema „Challenges in Implementing Information Security Policies" unter Univ.-Prof. Dipl.-Ing. DDr. Gerald Quirchmayr

1995-2000 Höhere Technische Bundeslehranstalt Ottakring (vormals Schellinggasse)
- Höhere Abteilung für Nachrichtentechnik

1991-1995 Allgemein bildende höhere Schule (Gymnasium)